Computers & Security 139 (2024) 103705

Contents lists available at ScienceDirect

Computers & Security

journal homepage: www.elsevier.com/locate/cose

Anomaly detection for space information networks: A survey of challenges, techniques, and future directions

Abebe Diro [a,*], Shahriar Kaisar [a], Athanasios V. Vasilakos [d], Adnan Anwar [b], Araz Nasirian [a], Gaddisa Olani [c]

[a] Department of Information Systems, RMIT University, 124 La Trobe Street, Melbourne, 3000, Victoria, Australia
[b] School of Information Technology, Deakin University, 221 Burwood Highway, Melbourne, 3125, Victoria, Australia
[c] School of Computing, Dire Dawa University, 1487, Dire Dawa, Ethiopia
[d] The Center for AI Research, University of Agder, on Lilletuns vei 9, Grimstad, 4879, Grimstad, Norway

ARTICLE INFO

Keywords:
AIndex terms - anomaly detection
Space security
Space anomaly detection
Cybersecurity
Space information networks
Dynamic space anomaly detection

ABSTRACT

Space anomaly detection plays a critical role in safeguarding the integrity and reliability of space systems amid the rising tide of threats. This survey aims to deepen comprehension of space cyber threats through space threat modeling, and meticulously examine the unique challenges of space anomaly detection. The survey identifies scalability, real-time detection, limited labeled data availability, concept drift, and adversarial attacks as key challenges based on thorough literature analysis and synthesis. By extensively exploring state-of-the-art anomaly detection techniques, the study evaluates their applicability, strengths, and limitations within space networks. Going beyond analysis, a notable contribution of this work involves integrating stream-based and graph-based methods, tailored to capture the intricate temporal and structural relationships inherent in space networks. This innovative hybrid approach holds promise for heightened detection accuracy and sets the stage for future research endeavors. As space threats continue evolving in both number and sophistication, this survey timely provides insights, recommendations, and a clear roadmap for researchers, engineers, and practitioners to fortify space anomaly detection mechanisms.

1. Introduction

The space industry, historically dominated by superpowers, is experiencing a paradigm shift. Anticipated to achieve a valuation surpassing $1 trillion by 2040, this ascension is a global phenomenon, involving not just established space-faring nations but also emerging economies (Barbaroux, 2016). This democratization, attributable to reduced launch costs and exponential advancements in computational paradigms like miniaturization and commercial off-the-shelf (COTS) components, has catalyzed a new era of space accessibility (Triscari, 2022; Cunningham et al., 2016). This evolution has catalyzed a proliferation in satellite-driven applications, encompassing domains from communication to meteorology and navigation (Beazley, 2020; Manulis et al., 2021; Nussbaum and Berg, 2020). The implications of this growth are profound and multifaceted. Beyond the creation of job opportunities and technological advancements, the space industry's expansion holds promise for societal benefits such as enhanced disaster response, global communication, economic growth, and environmental management (Johnson, 2019). Moreover, advancements in technology for space missions can drive scientific research, and enhance national security (Unal, 2019).

The interdisciplinary nature of space technology, intersecting with fields such as physics, engineering, environmental science, and law, adds complexity and richness to the industry (Borgia et al., 2023). The integration of Space Information Networks (SINs) with existing technologies, the emergence of privatized satellite networks, and the innovative use of Internet of Things (IoT) devices are just a few examples of how the space industry is evolving and intertwining with other sectors (Blount, 2017; Yue et al., 2022). Integration with IoT devices allows for environmental monitoring, maritime applications, military missions, and the development of interconnected devices and services (Blount, 2017; Yue et al., 2022). SINs, as shown in Fig. 1, encompass a network of systems such as satellites, unmanned aerial vehicles, airships, and other objects capable of receiving, processing, and transmitting real-time spatial and temporal information (Zhuo et al., 2021). However, this rapid expansion is not without risks and

* Corresponding author.
E-mail address: abebe.diro3@rmit.edu.au (A. Diro).

https://doi.org/10.1016/j.cose.2024.103705
Received 24 August 2023; Received in revised form 11 December 2023; Accepted 4 January 2024
Available online 10 January 2024

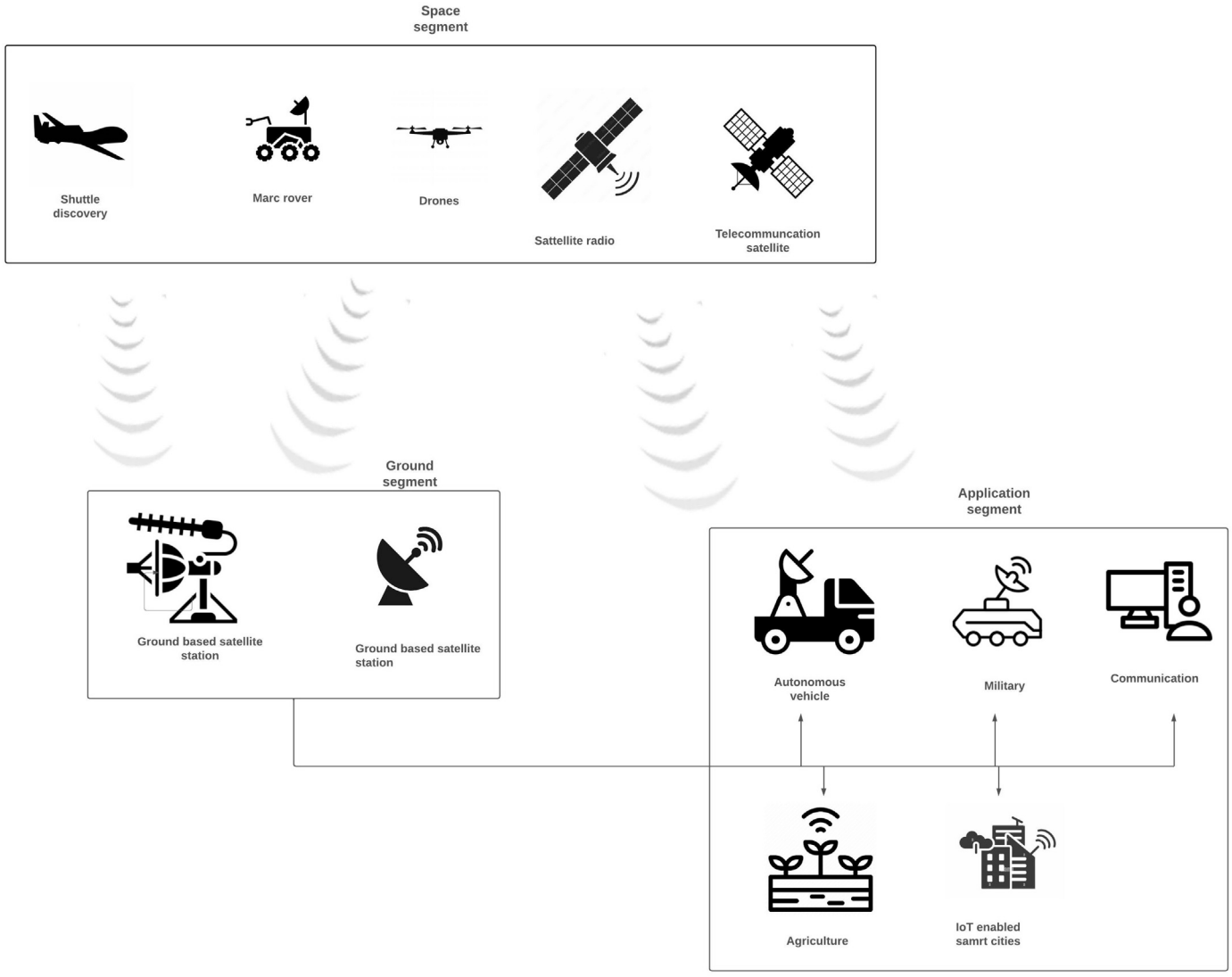

Fig. 1. A typical space information networks. Space Information Networks represent a convergence of space technology and information systems, promising to revolutionize numerous sectors, from defense to communication to transportation.

challenges. Cybersecurity has emerged as a critical concern, with the increasing reliance on satellites necessitating robust measures to ensure their protection (Hennecken, 2020). Alongside cybersecurity, satellites face vulnerabilities from a spectrum of threats, including space debris hazards, technical malfunctions, and potential natural interferences (Housen-Couriel, 2015; Falco, 2020). Disruptions in satellite operations could lead to compromised essential services and severe implications for global communication, navigation, and Earth observation systems. Prioritizing cybersecurity measures, specifically anomaly detection, becomes paramount to safeguard critical infrastructure, maintain service continuity, and mitigate risks from both cyber attacks and other environmental or technical anomalies (Livingstone and Lewis, 2016; Bailey, 2020).

1.1. Background and motivations

The rapid commercialization of space, combined with the commercialization of satellite launches, has given rise to a global ecosystem of privatized satellite networks, profoundly influencing both commercial and defense sectors (Mohamed and Chang, 2023). This evolution permeates every facet of the global economy and holds the promise of sustainable regional growth (Brukardt, 2022; Pavur and Martinovic, 2019). However, space security presents a unique set of challenges:

- **Single Point of Vulnerability**: SINs play a crucial role in sectors like communication, navigation, and defense. A single security breach can have cascading effects across these sectors. For instance, in 2019, a GPS spoofing attack in the Black Sea led to multiple ships inaccurately reporting their positions, causing significant navigational confusion. Such incidents underscore the need for robust protective measures (Caudill, 2020).
- **Complex Supply Chain and Extended Lifecycles**: The intricate supply chains of SINs, combined with their prolonged lifecycles, amplify the risk of malware infiltration. The 2020 SolarWinds cyberattack is a stark reminder of how adversaries can exploit complex supply chains to compromise critical systems, demanding meticulous security oversight throughout all phases (Oakley, 2020).
- **Integration of Commercial Off-the-Shelf Technology**: The use of COTS components in SINs, while cost-effective, can introduce vulnerabilities. These components, designed for general purposes and not specifically for the unique challenges of space, can be more susceptible to threats (Housen-Couriel, 2016). In 2020, a vulnerability was discovered in a widely-used COTS satellite communication system, which could allow hackers to intercept, manipulate, or block communications (Falco and Boschetti, 2021; Massimi et al., 2023; Llanso and Pearson, 2016).

- **Resource Constraints**: Space systems often operate under stringent resource constraints, including limited power, processing capabilities, and memory. Implementing sophisticated security measures can be challenging when they significantly impact system performance (Plotnek and Slay, 2022).
- **Extended Time Horizons**: The longevity of space missions demands cybersecurity measures that remain effective over extended periods, adapting to emerging threats and system wear (Baylon, 2014).
- **Limited Update Opportunities**: The infrequency of software updates for deployed space assets mandates that cybersecurity solutions be inherently robust and capable of autonomous adaptation (Pavur and Martinovic Sok, 2020).
- **High Latency Communications**: The communication lags inherent in space missions mean that cybersecurity systems must function autonomously, equipped with the intelligence to make on-the-spot decisions without awaiting ground directives (Al-Rodhan, 2020).
- **Size and complexity:** The sheer size and complexity of space systems pose another significant challenge. Satellites, for instance, consist of numerous components and subsystems, each with its own vulnerabilities and security risks (Holmes, 2022a).
- **Cosmic Influence and Hardware Anomalies**: Natural space phenomena can induce hardware glitches, like bit flips caused by cosmic rays. In 2018, a study highlighted how solar flares could potentially disrupt satellite communications, emphasizing the need to differentiate between these natural anomalies and genuine cyber threats (David Wright and Gronlund, 2005; Abeshu and Chilamkurti, 2018).
- **Technological evolution:** The rapidly evolving nature of space technology introduces a dynamic threat landscape. Security threats and vulnerabilities continually evolve, necessitating constant vigilance and adaptability from space organizations. Staying up-to-date with the latest threats and vulnerabilities is crucial to ensure the effectiveness of security strategies (Tsamis et al., 2021).

These challenges underscore the pressing need for advanced, autonomous, and adaptive security controls such as anomaly detection systems tailored to the unique environment and challenges of space operations. Traditionally space security has been viewed primarily as a military domain and relied on vulnerable black-box encryption (Pavur and Martinovic Sok, 2020). An anomaly detection system is used to detect patterns or sequences of patterns in networks or data that significantly deviate from normal behavior. They can play a pivotal role in accurately alerting users before cyber incidents spread and take control of the entire space information networks (Abeshu and Chilamkurti, 2018; Falco and Boschetti, 2021; Massimi et al., 2023; Llanso and Pearson, 2016).

Anomaly detection has become increasingly crucial in the context of space, as cyber attacks targeting space systems and infrastructures have grown in number and sophistication (Pearson, 2022). With the growing dependency of critical infrastructures, including communication, navigation, and surveillance, on space-based assets, the security of space systems directly impacts national security. The understanding and knowledge of space security, particularly in the domain of anomaly detection systems, are currently limited. This survey aims to make a significant contribution by providing a comprehensive overview of the state-of-the-art in space anomaly detection, encompassing advancements, challenges, and opportunities.

1.2. Main contributions

The paper by Tedeschi et al. (2022) underscores the importance of updating cybersecurity measures within space systems to combat evolving threats. Their survey categorizes security literature, explores specific research domains, and identifies emerging subjects for advancing satellite communications. However, it falls short in comprehensively addressing unique threats to space systems and does not delve into anomaly detection. To the best of our knowledge, the most recent survey on anomaly detection within Space Information Networks (SINs) was conducted by Zhuo et al. in 2021. While their research was noteworthy, it lacked an extensive examination of the practical security challenges unique to space systems and failed to cover the specific requirements of dynamic space anomaly detection. These challenges will be discussed in section 5. Specific contributions are:

- **Unique Space Threat Identification via Threat Modeling**: The survey meticulously examines assets, threats, vulnerabilities, defense mechanisms, and limitations within the Space Information Network (SIN) components—onboard computers, communication modules, and ground stations. This comprehensive analysis is crucial for shaping effective technological solutions addressing diverse security challenges encountered in space.
- **Requirements and Architectural Insight from Literature Analysis**: The survey delves deep into existing knowledge, identifying pivotal challenges in anomaly detection within dynamic space networks. It covers scalability, real-time detection, limited labeled data, concept drift unpredictability, and the rising threat of adversarial attacks. These insights pave the way for future research. Additionally, the article introduces a distributed architecture optimized for space data, ensuring efficient real-time anomaly detection even in complex networks.
- **Graph Stream Methods Fusion**: The survey advocates integrating stream-based and graph-based methodologies for dynamic space anomaly detection. By elucidating the mathematical underpinnings and algorithms of each approach, it highlights their potential in capturing the intricate temporal and structural complexities inherent in space networks.
- **Future-Focused Perspectives**: Beyond the present analysis, the survey provides forward-thinking insights. It engages in a robust discussion on the inherent challenges of dynamic space anomaly detection, offering actionable recommendations and potential research trajectories. From scalable algorithms to integration with other network analysis techniques, the article charts a roadmap for evolving more potent anomaly detection mechanisms tailored for the complex space environment.

1.3. Survey methodology

In this review paper, we utilized a systematic literature review (SLR) approach (Khalil et al., 2023; Chowdhury et al., 2021). The SLR framework has demonstrated its rigor in conducting comprehensive literature reviews. In Fig. 2, we present the search methodology adopted for this study, outlining the systematic process followed to gather relevant information and data. As shown in the Fig. 2, the survey encompassed esteemed databases such as Google Scholar and SCOPUS to compile a comprehensive array of scholarly articles, conference proceedings, and relevant publications pertaining to space systems and cybersecurity. In addition to database searches, the methodology involved an exploration of new articles to gain insights into contemporary issues and emerging trends within the field, supplementing scholarly discourse acquired from academic databases. A combination of keywords, including “space anomaly detection,” “space cybersecurity,” “space information security,” “satellite security,” and variations tailored to specific aspects, facilitated a broad search across literature sources, ensuring retrieval of diverse scholarly and industry-related works. The SCOPUS search retrieved 94 documents, among which 51 were pertinent to space cybersecurity, with only 14 falling within the area of anomaly detection. Similarly, the Google Scholar search yielded 117 documents, of which 95 were relevant to space cybersecurity, but only further 21 pertained to anomaly detection. While utilizing generic space cybersecurity

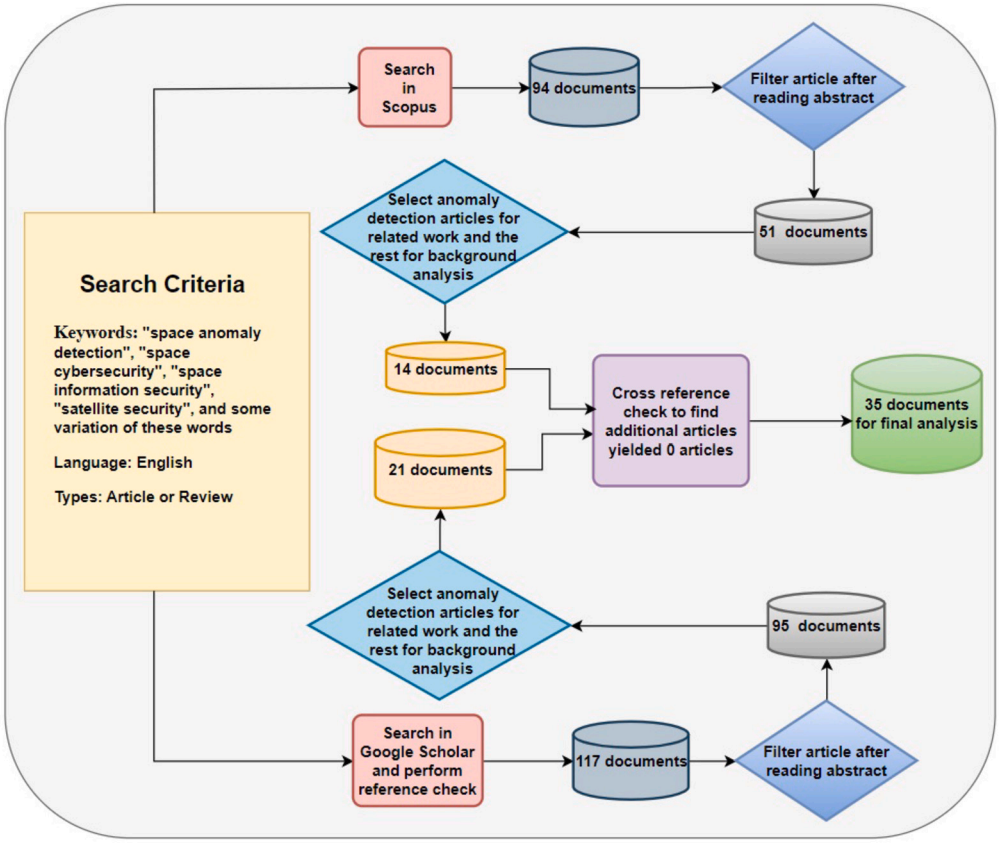

Fig. 2. Search methodologies to finalize the articles for analysis.

sources for background analysis to identify challenges and trends, we focused on the 35 articles anomaly detection-specific documents to address and elucidate key aspects related to this specific area within the broader domain of space cybersecurity. Ultimately, we examined the references of the articles, and no further relevant articles were identified through this process. The high degree of content overlap between SCOPUS and Google Scholar articles indicates a consistent presence of shared publications across these platforms in the field of space cybersecurity. The analysis of 111 generic space cybersecurity and 35 space anomaly detection articles was systematically reviewed to synthesize challenges, opportunities, and limitations in space cybersecurity, particularly focusing on space anomaly detection. Finally, this study delves into future research opportunities and outlines potential research questions by drawing upon the research findings from studies on space anomaly detection.

2. Historical space incidents and evolution

The history of space exploration is a testament to human ingenuity and perseverance. From the first satellite, Sputnik, launched in 1957, to the intricate networks of today, our journey in space has been marked by significant milestones (Rendleman and Ryals, 2013). However, as our capabilities have expanded, so have the threats. In the early days, challenges were primarily technical, focusing on achieving orbit or ensuring communication. Today, with the proliferation of SINs, the threats have evolved to encompass sophisticated cyber-attacks, espionage, and data breaches. Understanding this historical evolution is crucial, not just to appreciate our achievements but to anticipate and prepare for emerging threats. As we delve deeper into the vulnerabilities and threats in subsequent sections, this historical perspective will provide a foundation for our discussions.

2.1. Space incidents

The evolution of space security challenges can be delineated into six distinct phases, as summarized in Table 1 and Fig. 3. Each phase reflects the geopolitical and technological landscape of its era, revealing the dynamic nature of threats and the increasing complexity of safeguarding space assets.

Phase I (1960-70s): The 1960s marked the early stage of satellite technology, where discussions around the vulnerability of commercial missions to cyber attacks began to emerge. In 1962, a US congressional hearing specifically addressed the concerns regarding man-in-the-middle attacks, such as replay and jamming attacks, originating from the Soviet Union (Falco, 2018a). The potential threat posed by these attacks raised awareness of the security risks associated with satellite systems. However, despite these discussions, satellite hacking incidents remained relatively low in the following two decades, with the focus primarily shifting toward disputes related to satellite broadcasts. In this phase, there were ongoing disputes between the United States and the Soviet Union over satellite broadcast issues. The anti-communist transmissions by the USA provoked the Soviet Union to raise concerns about the jamming of illegal signals (Falco, 2018a). In 1972, the Soviet Union proposed a resolution to the United Nations (UN) to address the issue of jamming and illegal signals (Falco, 2018b). This dispute had a lasting impact on the establishment of norms and regulations surrounding jamming and eavesdropping attacks in the context of satellite communications (Baselt et al., 2022).

The discussions and events during Phase 1 set the foundation for future considerations and norms in satellite security. The congressional hearing in 1962 demonstrated the early recognition of the potential vulnerabilities of satellite systems to cyber attacks (Pavur and Martinovic Sok, 2020). The disputes between the United States and the Soviet Union highlighted the significance of addressing unauthorized

Table 1
Summary of Space threats, vulnerabilities, events and key takeaways.

Phase	Main Threats	Vulnerabilities	Main Events	Key Takeaway
Phase I	• Man-in-the-middle/Replay attacks • Jamming attacks	• Absence or weaknesses in signal encryption or authentication protocols, allowing interception	US congressional hearing on potential satellite vulnerabilities, disputes between the US and the Soviet Union over satellite broadcasts	The early recognition of potential vulnerabilities in satellite systems and the need for international cooperation to establish guidelines in space
Phase II	• Hacking • Signal injection attacks • Unauthorized access	• Flaws in communication protocols leading to signal injection/unauthorized access • Ground systems' security, such as inadequate access controls, enabling unauthorized system access	"Captain Midnight" hacking into HBO, signal injection attacks against "The Playboy" channel, German teenagers compromising NASA's missions	The increasing vulnerability of satellite systems to unauthorized access and the importance of proactive monitoring and detection mechanisms
Phase III	• Satellite-on-satellite interference • TV piracy • Unauthorized access	• Flaws in orbital configurations leading to satellite-on-satellite interference • Ground stations' flaws, such as inadequate access controls, leading to unauthorized access	Indonesia's satellite-on-satellite interference, satellite TV piracy using cryptography, unauthorized access to NASA's Goddard Space Flight Center by a Russian hacker	The emergence of adversarial actions in space and the importance of robust cybersecurity practices and secure communications protocols
Phase IV	• Signal hijacking • Malware • Anti-satellite weapons	• Flaws in Communication protocols allowing signal hijacking or eavesdropping • Ground systems' vulnerabilities, exploited by malware	Non-state actors like Falun Gong and Tamil Tigers engaging in signal hijacking, China's demonstration of an anti-satellite weapon, malware infecting orbiting systems	The increasing sophistication of offensive counter-space technology and the need for international cooperation and norms to prevent the weaponization of space
Phase V	• Cyber attacks • Signal intrusion • Espionage	• Communication protocols susceptible to cyber attacks or signal intrusion • Ground systems, exploited for espionage or gaining unauthorized access	Jamming attacks during the Arab Spring, signal intrusion by groups like Hamas, Turla group exploiting satellite internet signals, China's cyber-attacks on satellite ground stations	The escalating frequency and sophistication of cyber attacks on satellites, emphasizing the importance of international collaboration
Phase VI	• Escalating cyber attacks • Sophisticated adversaries • Non-state actors	• Satellite systems' security exploited by escalating cyber attacks, sophisticated adversaries, or non-state actors	Escalating cyber attacks targeting satellite systems, involvement of approximately 30 states and a rising number of non-state actors in space cyber threats	The urgent need for increased R&D to combat the growing and evolving threats to space assets

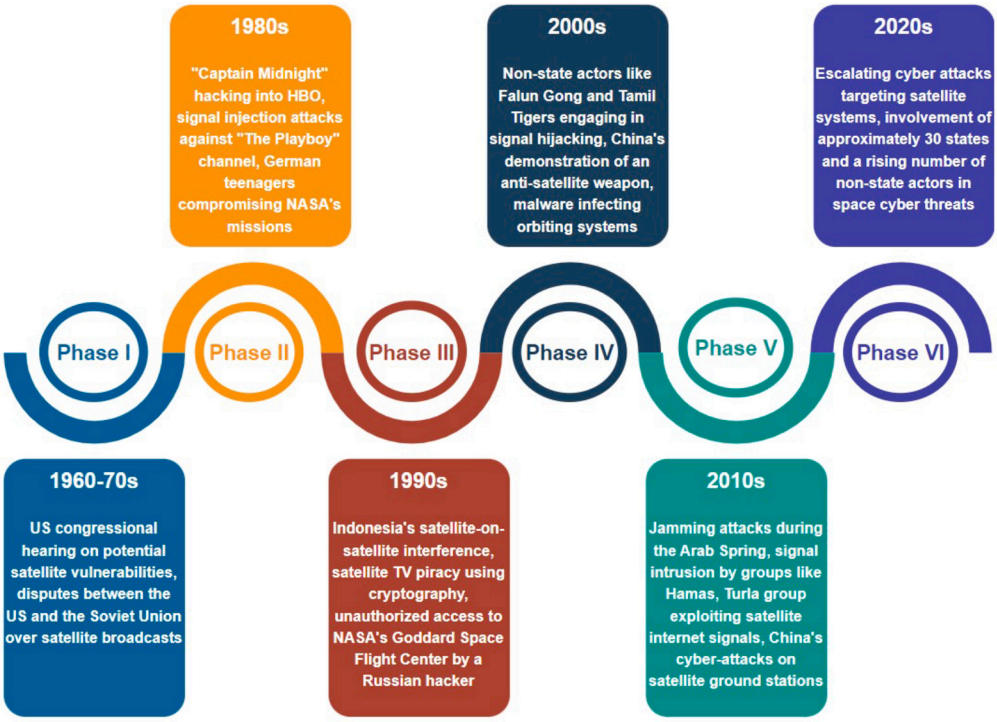

Fig. 3. Space Incidents Timeline. This figure presents a timeline of space incidents, segmented into six distinct phases, each highlighting the evolution of threats, notable incidents, and the implications for space cybersecurity.

signal interference and the need for international cooperation to establish guidelines for responsible behavior in space. The lasting impacts of these discussions on norms surrounding jamming and eavesdropping attacks emphasize the importance of developing robust security measures and international agreements to ensure the integrity and security of satellite communications.

Phase II (1980s): The 1980s marked a significant period for satellite security due to the increasing importance of satellite systems in industries such as telecommunications and earth observation. Vulnerabilities in satellite systems became evident, as demonstrated by notable incidents during this time. “Captain Midnight,” a man who hacked into an HBO television broadcast in 1986, replaced the signal with a message protesting the network’s signal-scrambling technology (Pavur and Martinovic, 2022). This incident highlighted the potential impact of satellite hacking and raised concerns about the security of satellite transmissions. Another incident involved signal injection attacks against the broadcasting channel “The Playboy” (Pavur and Martinovic, 2022). These incidents emphasized the vulnerabilities of satellite systems to unauthorized access, both in terms of transmissions and ground systems. Teenagers in Germany compromising NASA’s top-secret military missions also showcased the ethical considerations and consequences associated with such actions.

The incidents in the 1980s had important implications for space security and practices. They underscored the need for improved security measures and raised awareness about the potential threats to satellite systems (Ogden, 2022). Organizations were prompted to enhance security protocols and develop countermeasures to safeguard satellite transmissions and ground systems. The incidents also highlighted the importance of proactive monitoring and detection mechanisms for satellite security. Collaboration between satellite operators, government agencies, and security experts became essential to address evolving challenges and mitigate risks associated with satellite security breaches.

Phase III (1990s): The 1990s witnessed a significant increase in satellite usage and exploitation, leading to notable developments and challenges. The first known case of satellite-on-satellite interference occurred when Indonesia deployed a satellite to jam another satellite in a conflict over access to orbital slots (Fritz, 2013). This incident highlighted the potential for adversarial actions in space. Cryptography for satellite TV piracy also gained popularity, posing a significant challenge to media organizations. The adoption of cryptographic techniques enabled unauthorized access to satellite TV broadcasts, resulting in conflicts between media organizations and satellite pirates. Attacks against satellite ground stations further highlighted vulnerabilities in critical infrastructure. A Russian hacker gaining unauthorized access to NASA’s Goddard Space Flight Center control systems raised concerns about the security of space agency operations (Pavur and Martinovic Sok, 2020). Additionally, incidents involving space assets, such as the ROSAT X-ray telescope, highlighted the challenges of accurately attributing anomalies and the importance of reliable information and transparency.

The developments and challenges in the 1990s have significant implications for space security. The incidents of satellite interference, TV piracy, and unauthorized access underscore the importance of robust cybersecurity practices and secure communications protocols. The incidents also emphasize the complexity of space anomaly detection and the challenges associated with accurately assessing incidents. Reliable data sources, thorough investigations, and improved information sharing among stakeholders are crucial for understanding space anomalies and their causes (Liu et al., 2023b).

Phase IV (2000s): The early 2000s witnessed a significant increase in satellite incidents, introducing emerging trends and challenges to the space domain (Tanase, 2015; Gorman et al., 2009). Non-state actors, including Falun Gong, Tamil Tigers, and Iraqi insurgents, engaged in signal hijacking and eavesdropping activities, demonstrating an interest in exploiting vulnerabilities in satellite communications (Harrison et al., 2019). Attacks against satellite ground stations, such as the hijacking of NASA satellites’ signals linked to the Chinese government, highlighted risks associated with unauthorized access. A notable incident involved malware infecting orbiting systems through a Windows XP-based platform. China’s demonstration of an anti-satellite (ASAT) weapon in 2007 and targeting of US military satellite sensors using a

ground-based laser system in 2006 showcased the growing sophistication of offensive counter-space technology (Kaufman and Linzer, 2007).

The trends observed in the 2000s emphasize space security and stability concerns (Ogden, 2022). Non-state actors' actions underscore the importance of protecting satellite communications from unauthorized access and interference. Successful attacks against ground stations highlight the need for robust security protocols to safeguard critical infrastructure. The incidents involving malware and ASAT weapons underscore the evolving nature of threats in space and the importance of proactive measures to mitigate cyber risks and prevent the weaponization of space. International cooperation, agreements, and norms are necessary to maintain the peaceful use of outer space and ensure the long-term sustainability of space activities. Policymakers, space agencies, and stakeholders must prioritize space security, invest in resilient infrastructure, and enhance cybersecurity capabilities. Collaboration and dialogue among nations are crucial for developing comprehensive strategies, regulations, and best practices that promote responsible behavior in space and mitigate potential risks and threats (Robinson, 2016).

Phase V (2010s):The 2010s marked a significant shift in the space security landscape. Amidst the backdrop of global digitization and increasing geopolitical tensions, space assets became prime targets. The past decade has witnessed a significant increase in cyber attacks targeting space systems, signifying the evolving landscape of space security. Jamming attacks during the Arab Spring protests in 2010 demonstrated the potential for adversaries to disrupt satellite communications for their own purposes during times of political unrest (Pavur and Martinovic Sok, 2020). More sophisticated signal-related attacks, including signal intrusion by groups like Hamas, highlighted the need for robust security measures against signal interference. State actors, such as China, targeted ground stations and control systems, indicating strategic interests in compromising space infrastructure. The Turla group, affiliated with Russia, exploited satellite internet signals to steal sensitive data, showcasing the growing sophistication of cyber attacks in space (Pavur, 2021). Initiatives like the "Hack-A-Sat" competition and DEFCON's "aerospace village" have placed greater focus on satellite cybersecurity and the importance of robust practices in space operations.

The developments in the 2010s have significant implications for space security and policy (Varadharajan, 2022a). The increasing frequency and sophistication of cyber attacks in space necessitate resilient and secure space systems. International collaboration, information sharing, norms, and regulations are crucial to ensure the integrity and stability of space activities. Continuous research and innovation are necessary to stay ahead of emerging threats. Governments, space agencies, and cybersecurity experts must work together to develop effective defense mechanisms, encryption protocols, and intrusion detection systems tailored for space-based operations. The events of the past decade highlight the importance of international cooperation, situational awareness, and response capabilities to address space cybersecurity challenges (Pavur and Martinovic, 2021). Comprehensive strategies and measures must be implemented to safeguard satellites and protect critical services reliant on space infrastructure (Falco, 2019).

Phase VI (2020s): As we venture deeper into the 21st century, the threats to space assets have become more pronounced and sophisticated. Over the past six decades, there has been an escalating trend of cyber attacks targeting satellite systems, particularly in recent years (Holmes, 2022b). The scope and scale of these attacks have grown significantly, involving approximately 30 states and a rising number of non-state actors. The increasing frequency, complexity, and severity of these attacks highlight the evolving landscape of space security threats. Adversaries have become more sophisticated in their methods and techniques, posing a greater challenge to the security of satellite systems. Non-state actors have also demonstrated capabilities comparable to state actors, broadening the reach of cyber threats in space (Pearson, 2022).

The growing threat of cyber attacks on satellites raises significant concerns and underscores the urgent need for increased research and development to combat these threats (Boschetti et al., 2022b). Innovative technologies, robust encryption mechanisms, secure communication protocols, and intrusion detection systems specifically designed for space systems are essential (Abdulmonem et al., 2021). Collaboration among space agencies, cybersecurity experts, and academia is crucial to address evolving challenges and outpace potential adversaries. The implications of these cyber attacks extend beyond national security concerns. The reliance on satellites for critical infrastructure, including communications, navigation, weather monitoring, and remote sensing, means that successful attacks could have widespread societal and economic consequences. Therefore, protecting satellite systems is imperative to maintain the integrity and functionality of these vital services (Vessels et al., 2019).

Addressing the growing threat of cyber attacks on satellites requires a multi-faceted approach. It involves enhancing international cooperation, information sharing, and establishing norms and regulations to discourage malicious activities in space (Blount, 2023; Martin, 2023). Public-private partnerships should be fostered to combine expertise and resources in developing robust defenses and resilient space infrastructure. As the 2020s progress, continuous vigilance and proactive measures in space cybersecurity.

2.2. Analysis and implications

The vast expanse of space, once a realm of wonder and exploration, has transformed into a strategic domain, especially since the mid-20th century with the introduction of satellite technology. As we've ventured deeper into space, the technological advancements have brought forth a unique set of vulnerabilities and threats. A retrospective look at the history of space cybersecurity offers a lens through which we can understand the evolution of these threats and the incidents that have shaped our current understanding.

Early Satellites and Cold War Era (1950s - 1980s): The space age dawned with the Soviet Union's launch of Sputnik in 1957. This era was characterized by a superpower tug-of-war between the U.S. and the USSR. While the threats during this period were predominantly physical, such as the development of anti-satellite missiles, the seeds of espionage and intelligence warfare were sown, setting the stage for the cyber threats of the future.

The Digital Revolution and the Emergence of Cyber Threats (1990s - 2000s): The shift from analog to digital satellite systems marked a pivotal transition. As satellites became more intertwined with computer systems, they presented a broader attack surface for cyber adversaries. Notable incidents from this era, such as the 2007 cyberattack on a U.S. satellite and the 2008 malware infection of the ISS, served as stark reminders of the vulnerabilities inherent in the integration of space and digital technologies.

Modern Era of Space Cybersecurity (2010s - Present): The recent decade has witnessed an influx of commercial players like SpaceX, Blue Origin, and OneWeb into the space arena. While this has democratized space exploration, it has also broadened the threat landscape. State-sponsored cyber groups, with their sophisticated techniques, have increasingly targeted space assets for a myriad of reasons, from espionage to strategic advantage. The critical role of satellites in various sectors, from military to communication, has elevated their status to high-value targets.

Furthermore, the expansion of the space industry has led to a more intricate supply chain. This complexity was exploited in incidents like the 2020 SolarWinds hack, emphasizing the potential risks lurking within the supply chain itself.

Lessons from the Past: The evolution of space technology has been paralleled by the evolution of threats. The shift from analog systems to digital has not only enhanced capabilities but also introduced vulnerabilities. Events like the malware infection on the ISS underscore

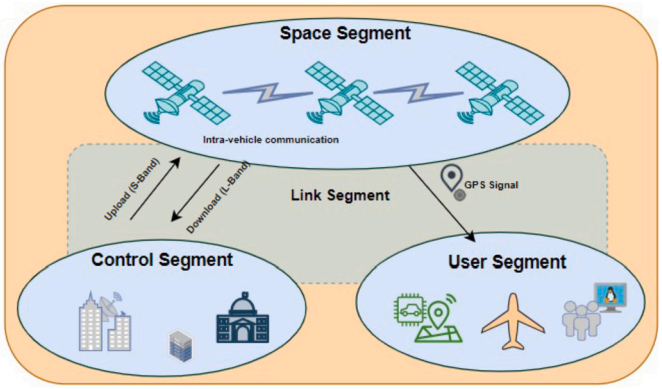

Fig. 4. Space segments. This figure provides a visual representation of the three primary segments in space operations: the space segment, the link segment, and the ground segment.

the intricate web connecting space and terrestrial systems, where a breach in one can jeopardize the other. Given the strategic significance of space, it remains a focal point for state-sponsored cyber activities. The international nature of space exploration necessitates global cooperation. Collaborative efforts in sharing intelligence, best practices, and establishing space norms can be pivotal in risk mitigation (Housen-Couriel, 2023).

3. Space threat modelling

Fig. 4 illustrates the three primary segments integral to space information systems: space, link, and ground. Despite the advancements in space technology, the space industry remains susceptible to cybersecurity threats across these segments. The digitization of space operations and the proliferation of satellite constellations have introduced vulnerabilities, notably remote code execution (Lemos, 2001), and software-related weaknesses (Eriksson and Giacomello, 2022). The integration of Commercial Off-The-Shelf (COTS) components, while expedient in reducing development time and costs, brings forth cybersecurity challenges. These components often lack inherent cybersecurity measures, potentially rendering them susceptible to cyber-attacks and unauthorized access, thus jeopardizing critical system functionalities (Jones, 2018).

3.1. Modelling approach

Threat modeling is a vital process that systematically evaluates potential risks and vulnerabilities, examining system assets, entry points, potential threat actors, and mitigation strategies (Javaid et al., 2012). It serves as a cost-effective means to anticipate system weaknesses, enabling stakeholders to focus strategically on enhancing system safety and security. Techniques like STRIDE, PASTA, LINDDUN, and Attack Trees reveal security issues, with STRIDE standing out as a mature and well-established method, providing security experts with a structured framework for thorough threat analysis and mitigation (Hasan and Hasan, 2022; Atmaca et al., 2022).

STRIDE encapsulates six key areas of security threats in computer systems and communication channels (Abuabed et al., 2023; Gupta et al., 2020). Spoofing involves illegitimate access using false identities, risking unauthorized changes to valuable assets. Tampering signifies intentional and unauthorized alterations to data or code. Repudiation manifests as an attacker's denial of involvement in malicious activities after compromising a system. Information Disclosure relates to obtaining restricted data. Denial of Service aims to block legitimate user access by overwhelming network resources. Lastly, Elevation of Privilege pertains to unauthorized acquisition of control or permissions. Within the space domain, various threats are identifiable through STRIDE threat modeling, as outlined in Table 2.

3.2. Space components, systems and assets

The standard communication model of a space system typically comprises several integral components that work together to facilitate satellite operations and data management:*satellite unit, ground station, Storage facility, manufacturing and development*, as shown in Fig. 5. Each of these subsystems contains several assets that enable them function. Assets refer to valuable elements, whether tangible or intangible, that are integral to space systems functionality and operation (Hasan and Hasan, 2022). These assets become prime targets for potential attackers whose aim may involve accessing, altering, or destroying them. In the initial phase of threat modeling, identifying these assets becomes imperative.

The satellite unit comprises several interconnected subsystems, as outlined in the first component in the Fig. 6, include RF Modulation and Demodulation (part of the Communication Subsystem), Telemetry, Tracking, and Command System (TT&C), Command and Data Handling System (C&DH), Attitude and Orbit Control System (AOCS, ADCS), and Mission Equipment, such as imaging units or specialized instruments.

The Communication subsystem, an integral part of the Communication Subsystem, facilitates the conversion of digital signals from the satellite's internal systems into radio signals for transmission and vice versa (Lewis and Livingstone, 2016). It handles the modulation and demodulation of radio frequency signals essential for communication with ground stations and inter-satellite communications. The TT&C subsystem plays a pivotal role in the satellite's operation by collecting data from onboard sensors, tracking its position and trajectory, and facilitating command transmission to the satellite from ground control. It encompasses telemetry, responsible for monitoring the satellite's health and performance, and tracking systems that determine the satellite's precise location and orbit (Eriksson and Giacomello, 2022). Moreover, the Command and Data Handling System (C&DH) manages incoming commands from ground control, processing and executing these instructions while handling data storage and processing for various satellite operations. Simultaneously, the Attitude and Orbit Control System (AOCS, ADCS) governs the satellite's orientation, attitude, and orbital maneuvers, ensuring precise control over its position and trajectory in space. The Mission Equipment subsystem involves mission-specific instruments or payloads, like imaging units, that perform specialized tasks or experiments as per the satellite's mission objectives. These components, interconnected by an internal bus like the Controller Area Network (CAN), enable efficient communication and coordination among subsystems, ensuring synchronized operations and effective management of the satellite's functionalities throughout its mission lifespan. Space subsystem assets are listed in Table 3.

Ground subsystems, meanwhile, comprise Earth-based facilities like RF modulation and demodulation (communication subsystem), Network operation system, Orbit control system, Satellite control system, Mission control system, Record, as shown in the second component of Fig. 6.

The communication (RF Modulation and Demodulation) subsystem handles the encoding and decoding of radio frequency signals, employing techniques like AM, FM, or PM for efficient communication between satellites and ground stations. Network Operation Systems manage and coordinate receiving stations, facilitating data transmission and command relays between satellites and control centers (Tanase, 2015). The Orbit Control System is responsible for maintaining and adjusting a satellite's orbit, employing propulsion, navigation, and guidance systems to regulate its position and trajectory. Simultaneously, the Satellite Control System oversees the satellite's internal functions, including subsystem management, payload operations, power distribution, and health monitoring. Mission Control Systems serve as the nerve center, where human operators strategize, execute, and supervise mission activities. These operators monitor telemetry, analyze data, and make critical decisions regarding satellite operations to ensure mission success. Additionally, the Record System manages the storage, retrieval, and

Table 2
Potential Threats in the STRIDE Model for Space Systems.

Category	Potential Threats in Space Systems
Spoofing	- Impersonation of satellite systems or ground stations. - Falsification of satellite identification or credentials. - Masquerading as authorized space entities.
Tampering	- Unauthorized alteration or modification of satellite data or telemetry. - Manipulating satellite configurations or navigation settings. - Modifying satellite software or code without proper authorization.
Repudiation	- Denial of unauthorized satellite access events. - Non-repudiation failure during critical satellite operations. - Inability to prove unauthorized satellite commands or alterations.
Information Disclosure	- Unauthorized access to sensitive space mission data. - Exposure of confidential mission details to unauthorized entities. - Data leaks or breaches compromising mission-critical information.
Denial of Service (DoS)	- Flooding satellite systems or ground stations with excessive requests, rendering them unusable. - Disrupting satellite services critical for communication or navigation. - Exhausting space system resources, affecting overall functionality.
Elevation of Privilege	- Unauthorized escalation of user privileges within satellite control systems. - Gaining elevated access levels or permissions beyond authorized protocols. - Exploiting vulnerabilities to achieve higher access rights within space systems.

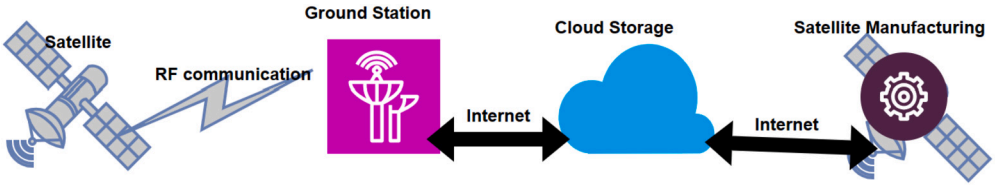

Fig. 5. A standard space Interaction system.

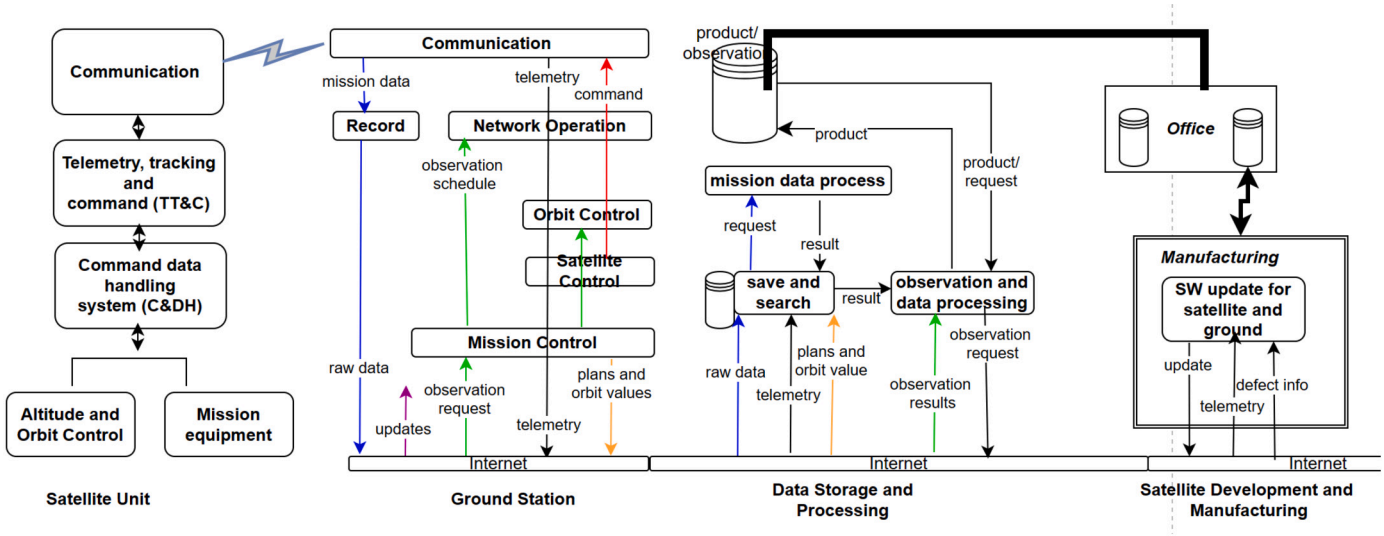

Fig. 6. Space communication subsystems and interactions.

archiving of mission-critical data, preserving telemetry logs, command records, and scientific information collected during the mission for future reference and analysis (Falco, 2018b). These integrated subsystems collectively form the backbone of space missions, enabling communication, data acquisition, and operational control between satellites and ground stations. Ground subsystem assets are listed in Table 4.

Utilizing the capabilities of the **cloud** is instrumental in space systems, offering an avenue for storing mission-critical data and product information while facilitating their processing. Organizations have the flexibility to employ a combination of cloud-based storage solutions alongside on-site facilities and dedicated data centers for the comprehensive management and processing of data related to space missions. This subsystem, as shown in the third component of Fig. 6, plays a pivotal role in both the operational and manufacturing aspects of space systems, ensuring seamless data management, processing, and accessibility. The assets encompassed within this system are elaborated in Table 5, highlighting various components and resources utilized for efficient data handling, storage, and processing in the context of space missions.

Manufacturers and developers actively engage with space systems by employing cloud-based storage solutions as a pivotal platform for managing and implementing software updates, as shown in the fourth

Table 3
Space Segment Subsystem Components and assets.

Subsystem	Hardware	Software	Data	Infrastructure	Other Components
Communication	Antennas, transmitters, receivers	Signal processing software	Telemetry data	Communication infrastructure	-
Telemetry, Tracking, and Command	Telemetry equipment, antennas	Command execution software, control algorithms	Telemetry, tracking, command data	Ground station network	Sensors, ranging systems
Command and Data Handling	Onboard computers, data buses, storage devices	Data processing software, control algorithms	Processed and stored mission-specific data	Onboard interfaces	Data recorders, solid-state drives
Altitude and Orbit Control	Gyroscopes, sensors, actuators	Control algorithms, guidance software	Orbit and altitude control data	Control systems for orientation and orbit	Thrusters, reaction wheels
Mission Equipment	Scientific payloads, imaging systems	Mission-specific software	Scientific, imaging, or mission-specific data	Ground-based facilities for data processing	Specialized instruments for mission objectives

Table 4
Ground Subsystems and assets.

Ground Subsystem	Hardware	Software	Data	Infrastructure	Other Components
Communication	Ground station equipment, antennas	Signal processing software	Received signal data	Ground station network, communication infrastructure	-
Network Operation System	Receiving and control station hardware	Network operation software	Network operational data	Control station facilities, network infrastructure	-
Orbit Control System	Control station equipment	Orbit control software	Orbit adjustment data	Control station infrastructure	-
Satellite Control System	Control station hardware, interfaces	Satellite control software	Satellite operational data	Control station facilities, communication infrastructure	-
Mission Control System	Control center hardware, interfaces	Mission control software	Mission-specific data	Mission control center infrastructure	Control consoles, monitoring equipment
Record	Storage devices, archival systems	Record management software	Archived mission data	Data storage and archival facilities	Data retrieval systems, data management tools

Table 5
Components of Cloud Storage Subsystem and assets.

Cloud Storage Subsystem	Hardware	Software	Data	Infrastructure	Other Components
Mission Control Data Processing System	Cloud servers, storage devices	Data processing software	Mission control-related processed data	Cloud infrastructure, virtual servers	Processing algorithms, analytics tools
Observation Request and Data Distribution Processing System	Cloud servers, storage devices	Request handling software	Observation requests, distributed data	Cloud-based databases, networking infrastructure	Request scheduling systems, data distribution tools
Mission Data Database	Cloud storage, databases	Database management software	Mission-specific data storage	Cloud-based database systems, data management tools	Data indexing systems, retrieval algorithms
Product Database	Cloud storage, databases	Database management software	Processed and archived product data	Cloud-based database systems, data management tools	Product categorization systems, metadata management

component of Fig. 6. This process encompasses the transmission, storage, and retrieval of software patches, upgrades, and modifications for both ground-based infrastructure and equipment integrated within satellites orbiting in space (Falco, 2018a). Leveraging cloud storage facilitates seamless access to a centralized repository, enabling efficient distribution and deployment of critical updates across the entire network of satellite systems and associated ground stations. This approach ensures that the software deployed in space systems remains current, enhancing functionality, security, and overall system performance while adhering to the unique constraints of space missions. Assets in this component are listed in Table 6.

3.3. STRIDE space cyber threats

The cyber threat landscape targeting space information systems has become increasingly complex and perilous. The surge in space-related activities and reliance on satellite technology has amplified the risk of cyber threats. The prominent cyber threats to space information systems can be listed as follows based on STRIDE model (Yue et al., 2022; Tedeschi et al., 2022):

Spoofing: Space systems face significant threats from spoofing tactics, which involve deceitful attempts to gain unauthorized access by using false identities or counterfeit credentials (Pavur and Martinovic, 2019). These threats pose a severe risk to satellite control systems, as attackers employ various deceptive tactics to breach security measures. By assuming the identities of legitimate entities or transmitting falsified command signals, attackers can infiltrate satellite control systems, thereby manipulating their operations (Ahmad et al., 2022). Orbital spoofing, a particularly concerning tactic, targets critical orbital data necessary for proper satellite functioning. Attackers manipulate this information, potentially compromising satellite positioning, navigation systems, and communication processes (Cyr et al., 2023). For instance, malicious actors exploit authentication vulnerabilities through techniques such as phishing or replay attacks, mimicking valid communications (Salkield et al., 2023). Furthermore, weaknesses in radio frequency communication links between satellites, ground stations, and user terminals provide opportunities for attackers to intercept, manip-

Table 6
Manufacturing Subsystem Components and assets.

Manufacturing Subsystem	Hardware	Software	Data	Infrastructure	Other Components
Office Automation System	Office computers, networking equipment	Office automation software	Administrative and management data	Office network infrastructure	Office productivity tools, communication systems
Manufacturing System	Manufacturing equipment, hardware tools	Software update tools	Satellite and ground station updates	Manufacturing facilities, update servers	Version control systems, update scheduling tools

ulate, or disrupt signals, thus undermining the system's integrity and security (Forester, 2015).

An alarming instance involves the manipulation or falsification of GPS signals (Yue et al., 2022; Elmarady and Rahouma, 2021; Falco et al., 2021) using ground station antennas. This deceptive practice aims to mislead satellite communication or navigation systems, resulting in inaccurate spatial information. As a consequence, erroneous positioning or disrupted communication between satellites and ground stations may occur, potentially jeopardizing critical operations reliant on precise spatial data transmission (Falco, 2020). These exploitations of authentication mechanisms, communication protocols, and overall security vulnerabilities within satellite systems underscore the urgent need for robust authentication and encryption protocols to counteract spoofing attacks in space systems (Mirchandani and Adhikari, 2020; Vivero, 2013).

Tampering: Tampering threats in space systems involve unauthorized changes to critical components like data, configurations, and hardware, aiming to disrupt satellite operations, compromise data integrity, or gain system control (Calabrese, 2023). Attackers might modify satellite settings, causing operational disruptions or data integrity compromises. Manipulating satellite control software could lead to transmitting incorrect commands to spacecraft, potentially altering orbits or undermining mission objectives. Additionally, unauthorized software updates and hardware manipulation are significant concerns. Manipulating command signals sent to satellites exploits vulnerabilities in authentication mechanisms, software update procedures, or satellite control protocols. Orbital Path Tampering poses a unique threat, disrupting a satellite's intended trajectory or altering its orbital path, risking critical operations such as communication, navigation, or scientific research (Tedeschi et al., 2022). Physical attacks using Kinetic Anti-Satellite (ASAT) weapons are designed to disable or destroy satellites through direct collisions or fragmentation, causing space debris and damaging operational satellites (Tedeschi et al., 2022). Supply chain attacks involve targeting software, hardware, or firmware components, introducing compromised or counterfeit components to gain unauthorized access or control. Malware propagation across satellite constellations poses challenges, requiring robust security measures, including supply chain integrity and fortified communication protocols, to mitigate risks and curb malware spread (Fick et al., 2022). The vulnerabilities within space systems can be delineated across various segments crucial to satellite operations (Falco et al., 2021; Falco, 2020).

Repudiation: Although uncommon, repudiation threats in space systems involve malicious activities carried out within the system, followed by attackers denying involvement or disputing the legitimacy of their actions. These threats manifest as unauthorized modifications to satellite data or system configurations, followed by the denial of any such alterations by the attackers. Within space systems, non-repudiation failures could lead to challenges in verifying or authenticating the actions performed, potentially enabling attackers to exploit the system without being held accountable. This creates ambiguity regarding the legitimacy of system alterations or manipulations, complicating the process of attributing responsibility for unauthorized activities within space systems. Attackers exploiting repudiation threats aim to evade detection and accountability by leveraging weaknesses in logging mechanisms, digital signature verification processes, or audit mechanisms within satellite systems. By exploiting these vulnerabilities, attackers attempt to manipulate or alter system logs, erase traces of their activities, or forge digital signatures to disown their actions, making it challenging to attribute unauthorized activities accurately (Hasan and Hasan, 2022). Strengthening digital forensics capabilities, enhancing logging mechanisms, and implementing robust audit trails are crucial countermeasures to mitigate repudiation threats in space systems.

Information Disclosure: Information disclosure threats in space systems entail the unauthorized access to sensitive space-related data, potentially resulting in the exposure of confidential information to unauthorized entities or leading to data breaches (Varadharajan, 2022b). Attackers in this domain aim to exploit vulnerabilities, seeking access to sensitive information stored within satellites or transmitted through satellite communication channels. For example, unauthorized access to satellite imagery or confidential data exchanged between ground stations and satellites has the potential to compromise national security or expose sensitive research information. These threats pose significant risks to data integrity, confidentiality, and national security within space systems. Notably, state-sponsored or industrial cyber espionage activities present notable risks to space information systems (Knez et al., 2016).

To achieve their goals, attackers employ a spectrum of sophisticated techniques, including packet sniffing, injection attacks, or man-in-the-middle attacks, targeting the interception and access of confidential information traversing satellite communication links. These tactics capitalize on exploiting weaknesses in encryption protocols, insecure data transmission practices, or inadequate access controls, posing substantial risks to the security and integrity of space-related data (Falco et al., 2023).

Denial of Service (DoS): Denial of Service threats in space systems focuses on rendering satellite systems unavailable by overwhelming them with excessive traffic or disrupting their services (Thangavel et al., 2022). Malicious actors employ various tactics, flooding satellite communication channels with an overwhelming volume of data, effectively rendering them unusable for legitimate users. These disruptions in satellite services could significantly impact critical operations such as communication, navigation, or remote sensing, posing substantial risks to industries heavily reliant on satellite technologies for their day-to-day operations. One common technique employed by attackers is signal jamming, which involves interfering with satellite signals to cause service disruptions or communication failures. These tactics capitalize on vulnerabilities within satellite communication protocols or utilize specialized equipment to disrupt or overload satellite services (Javaid et al., 2012). Attackers employ tactics such as signal jamming to disrupt satellite services, impacting critical operations like communication, navigation, or remote sensing, causing Dos (Forester, 2015).

Elevation of Privilege: Elevation of Privilege threats focus on unauthorized access escalation or exploiting system vulnerabilities to gain elevated control over satellite systems. Attackers leverage weaknesses within satellite systems to escalate their privileges, gaining unauthorized access to critical functionalities or controls. For instance, compromising ground station credentials to gain unauthorized control over satellite operations could result in extensive disruptions or manipulations of satellite functionalities (Boschetti et al., 2022a). For instance, insider threats with malicious intent, negligent behavior, or unintentional actions can result in unauthorized access, data breaches, or system disruptions (Zatti, 2017). Unauthorized credential escalation in-

Table 7
STRIDE Categories, Threats, Vulnerabilities, and Descriptions in Space Systems.

STRIDE Category	Threat	Vulnerability	Description
Spoofing	Orbit Spoofing	Susceptibility of navigational systems	False data leading to misalignment in orbits.
Tampering	Manipulating Orbital Paths	Unauthorized access to alter orbits	Illegitimate access to satellites altering their intended orbits, risking collisions or hazardous trajectories.
Tampering	Laser Weapons, Particle-Beam Weapons	Lack of defense against directed energy weapons	Potential use of directed energy weapons to tamper with or disable space assets.
Tampering	Radio Frequency Interference	Insecure signal protocols	Signals between satellites being exploited to manipulate or disrupt communication among assets.
Tampering	Solar Radiation and Cosmic Ray Interference	Radiation-induced electronic faults	Cosmic radiation in space induces electronic faults, creating potential vulnerabilities exploitable by cyber assailants.
Tampering	Supply Chain Compromise	Compromised components during manufacturing	Compromised components or software during manufacturing can serve as entry points for cyber attacks on space systems.
Tampering	Unauthorized Ground Station Access	Physical intrusion at ground stations	Physical intrusion or sabotage at ground stations disrupting communications, compromising sensitive data, or interfering with command functions.
Denial of Service	Space Debris Collision	Orbital collision with debris	Cyber threats redirecting satellites into collision courses with space debris, potentially leading to physical damage.
Information Disclosure	Eavesdropping and Signal Interception	Unauthorized access to sensitive data	Unauthorized access to sensitive data transmitted between ground stations and satellites compromising mission-critical information.
Tampering	Interference with Signal Integrity	Deliberate signal interference	Deliberate interference with satellite signals disrupting communications or navigation systems.
Denial of Service	Ground Terminal Disruption	Overloading communication channels	Overloading communication channels or networks with excessive traffic rendering space systems inaccessible or disrupting operations.
Tampering	Unauthorized Software Updates	Vulnerabilities in satellite systems	Vulnerabilities in satellite systems exploited to gain control, potentially altering its orbit, disrupting its functions, or causing physical damage.
Tampering	Physical Intrusions and Hardware Manipulation	Physical sabotage at ground stations	Physical intrusion or sabotage at ground stations disrupting communications, compromising data, or interfering with commands.
Elevation of Privilege	Insider Threats	Malicious actions by insiders	Malicious or unintentional actions by insiders compromising sensitive information or systems.
Information Disclosure	Cyber Espionage	Gathering sensitive information	Attempts to gather sensitive information about satellite operations, designs, or capabilities through cyber espionage.
Tampering	Network Infrastructure Vulnerabilities	Inadequate cybersecurity policies	Inadequate regulations or policies regarding cybersecurity in space systems creating loopholes and vulnerabilities.
Repudiation	Denial of Service or Data Manipulation	Lack of proper tracking or authentication	Potential instances of denying service or manipulating data without leaving evidence of having performed the action.

volves abusing legitimate credentials to gain additional privileges or access within satellite networks. These tactics exploit vulnerabilities in authorization mechanisms, software, or supply chain security, allowing attackers to gain unauthorized control over satellite operations. The Ground Stations that facilitate communication with satellites also exhibit vulnerabilities. These vulnerabilities often reside within the network infrastructure supporting these stations, allowing unauthorized access or manipulation by malicious actors. Physical access to hardware and software components within ground stations poses direct risks, enabling attackers to exploit vulnerabilities and potentially gain control over critical functionalities. Weaknesses in operational devices or flaws in data processing systems serve as gateways for unauthorized access or manipulation by malicious actors which leads to privilege escalation.

Inherent vulnerabilities exist in different Space Information Network (SIN) components, such as satellite onboard computer systems, communication links, and ground stations, as illustrated in Fig. 4 and summarized in Table 7.

3.4. Attackers and attack scenarios

In this section, we delve into the profiles of potential attackers within the space systems domain, exploring their motivations, skill sets, and available resources. Additionally, we outline various attack scenarios orchestrated by these threat actors, offering insights into the diverse range of cyber threats and vulnerabilities prevalent within this complex ecosystem.

3.4.1. Attackers

As shown in Table 8, space cybersecurity faces multifaceted threats from diverse attacker types, each driven by distinct motivations, employing varied attack methodologies, and possessing specific skills and resources (Knez et al., 2016).

Military entities, aiming for space control, leverage Anti-Satellite (ASAT) weapons and tactics like satellite jamming or physical destruction. They possess specialized weapon capabilities and strategic military resources. Such actions could severely disrupt communication and navigation systems, leading to a loss of critical satellite control, critically impairing navigational systems, and jeopardizing overall space operations (Manulis et al., 2021; Falco et al., 2023). Simultaneously, intelligence agencies focus on counter-intelligence and technology theft. They have sophisticated surveillance and cyber espionage skills, enabling them to breach crucial systems such as satellite telemetry and communication links.

Organized crime's involvement in eavesdropping presents risks of data theft and disruptions to communication networks. They possess skills in hacking and data interception. Similarly, terrorist groups, with moderate ASAT capabilities, aim to broadcast messages and gain notoriety (Pavur and Martinovic, 2022). They possess moderate weapon capabilities and propaganda dissemination skills. Their tactics could result in communication disruptions and the dissemination of terror propaganda, potentially causing public panic and disrupting essential services reliant on satellite communications. Commercial competitors resort to sabotage and technology theft, potentially compromising proprietary information and disrupting R&D operations. They have resources to fund cyberattacks and technological capabilities (Hasan and Hasan, 2022).

The impact extends further as political activists engage in message broadcasting and social media manipulation, potentially leading to misinformation dissemination and social instability. They possess skills in social media manipulation and message broadcasting. Simultaneously, nation-state actors, pursuing strategic goals, threaten political instability, breach of sensitive information, and disruptions to vital systems, endangering national security and stability. They possess advanced cyber warfare capabilities and significant resources (Boschetti et al., 2022a).

Table 8
Various attacker types, their motivations, methods, skills, targets, and impact.

Attacker Type	Motivation	Attack Methods	Targeted Systems/Assets	Skills and Resources	Impact Assessment
Military	Seeks space control and possesses Anti-Satellite (ASAT) weapon capabilities.	Satellite jamming, Physical destruction of satellites	Communication systems, Navigation systems, Satellites in orbit	Advanced technical expertise in space technology, access to ASAT weaponry	Disruption of communication, Potential loss of satellite control
Intelligence	Aims for counter-intelligence, technology theft, and eavesdropping activities.	Cyber espionage, Data interception	Satellite telemetry, Communication links, Data transmission systems	Advanced hacking skills, sophisticated surveillance capabilities	Breach of sensitive data, Communication interception
Third-party Supplier	Engages in sabotage due to their moderate access to specific components or systems.	Insertion of faulty components, Software manipulation	Hardware components, Software systems	Insider knowledge, access to supply chains	System malfunctions, Compromised system integrity
Organized Crime	Primarily involved in eavesdropping and occasionally ransom-related activities.	Data interception, Blackmail	Communication networks, Data centers	Cyber extortion tactics, hacking skills	Data theft, Potential service disruption
Terrorist	Possesses low to moderate capabilities for Anti-Satellite (ASAT) weapons and aims for message broadcasting and notoriety.	Cyberterrorism, Propaganda dissemination	Satellite navigation, Communication networks	Basic hacking skills, social engineering expertise	Communication disruption, Terror propaganda dissemination
Commercial Competitors	Engages in sabotage and technology theft to gain competitive advantages in the market.	Data theft, Sabotage	R&D systems, Proprietary technology	Industrial espionage tactics, access to corporate networks	Compromised proprietary information, Disrupted R&D
Individual Hackers	Motivated by seeking notoriety and personal challenges, often having limited capabilities.	Phishing attacks, Exploiting system vulnerabilities	User data, Access credentials	Basic hacking knowledge, access to hacking tools	Data breaches, System compromise
Political Activists	Primarily focused on message broadcasting with very limited capabilities for cyber activities.	Social media manipulation, Online campaigns	Public perception, Social media platforms	Social engineering tactics, online influence	Dissemination of misinformation, Online unrest
Nation-State Actors	Aim for strategic goals such as political influence, espionage, and economic disruption.	Advanced persistent threats, Cyber espionage	Critical infrastructure, Government networks	State-sponsored resources, cyber warfare capabilities	Political instability, Breach of sensitive information
Hacktivists	Engage in cyberattacks for political or social reasons, promoting their ideological agendas.	Website defacement, DDoS attacks	Government websites, Public services	Basic hacking skills, access to DDoS tools	Disrupted online services, Loss of website credibility
Insider Threats	May exploit their authorized access to commit cyber sabotage, espionage, or data theft.	Unauthorized data access, System manipulation	Classified data, Internal systems	Insider access, knowledge of system vulnerabilities	Data leaks, System sabotage
Script Kiddies	Often young and inexperienced hackers who use pre-written scripts to breach systems for fun or experimentation.	Exploiting known vulnerabilities, Simple malware attacks	Low-security systems, Public-facing servers	Basic hacking scripts, access to hacking forums	System compromise, Unauthorized access
State-Sponsored Hackers	Receive backing from a nation-state to conduct cyber operations for political, economic, or military advantage.	Sophisticated malware, Covert operations	Critical infrastructure, Military systems	State-sponsored resources, advanced cyber warfare capabilities	Serious national security threat, Economic disruptions

Internally, insider threats and script kiddies both pose risks of data leaks, system sabotage, and potential disruptions to operational systems. Insider threats have authorized access and knowledge of internal systems, while script kiddies possess basic hacking skills and rely on pre-written scripts. Lastly, state-sponsored hackers, with sophisticated capabilities, pose severe national security threats and economic disruptions. They have access to extensive resources and employ sophisticated cyber warfare techniques, compromising critical infrastructure and impacting geopolitical stability and economic vitality (Zatti, 2017; Book, 2006).

These diverse impacts from different attacker types highlight the multi-faceted threats encountered in space cybersecurity. Robust defense strategies, including encryption, access controls, system monitoring, and diplomatic actions, are essential to safeguard space infrastructure against these varied and potent threats

3.4.2. Attack scenarios

Numerous threat and attack scenarios can be conceptualized within space systems, each posing potential risks to the integrity and security of these complex networks. In this section, we delineate six distinct threat and attack scenarios within the intricate space network ecosystem, aiming to exemplify the diverse range of vulnerabilities and potential challenges encountered in safeguarding these critical systems.

1. **Scenario 1**: Within the manufacturing office, a targeted social engineering attack compromised an employee's computer, enabling remote access to sensitive data related to altitude control and mission equipment management. This breach allowed cyber intruders to extract confidential information, possibly involving industrial espionage or cyber intelligence within the manufacturing and development facility. Exploiting this stolen data, attackers manipulated the satellite-to-ground station communication using spoofing and replay attacks to take control of the uplink data for the satellite unit. With unauthorized access, they sent commands to the satellite, executing actions not authorized by legitimate personnel. As a result, these unauthorized commands could potentially disrupt satellite orbit control, leading to significant operational disruptions and hazardous situations.
2. **Scenario 2**: In the manufacturing facility, espionage tactics were employed to compromise the automation office computer, utilized by both manufacturing and development teams for software updates, through malware infiltration. Exploiting this access, hackers planted a backdoor within the software update system. Consequently, malware infiltrated computers integral to satellite software updates, integrated with the office system. This breach severely disrupted remote operations from ground control, leading to a loss of regular command and management capabilities for the satellite and mission equipment. The compromise not only undermines the integrity of satellite operations but also poses substantial challenges in maintaining essential control and functionality.
3. **Scenario 3**: In the data storage and processing facility, unauthorized single-board computers were installed within the organization, followed by hackers gaining unauthorized access via the Internet. This illicit access facilitated lateral movement across the network segments, spanning from mission data and satellite control communication to breaching the office automation system in the manufacturing sector. The unauthorized access extended further into the manufacturing facility servers, navigating through non-segmented networks. This progression allowed intruders to reach critical ground stations involved in satellite and mission control operations. Following a prolonged period of internal activity, multiple servers crucial for satellite operations experienced malfunctions, leading to an extended loss of control over the satellite. This disruption persisted due to the breakdown of various servers integral to satellite operations, significantly impacting telemetry, tracking, command systems, and command data handling.
4. **Scenario 4**: In the manufacturing domain, hackers discreetly embed Advanced Persistent Threats (APTs) within circuit boards utilized in altitude orbit controllers, offering these compromised boards at a reduced cost to satellite developers intending to create constellations comprising numerous units. Despite undergoing inspections, these APT-infected boards manage to slip through acceptance checks conducted by manufacturing personnel. They evade detection during unit inspections and system evaluations on the ground as specific conditions required for detection are not met. Following launch, the activated APTs, triggered under specific conditions, disrupt normal satellite control, placing the entire satellite constellation at risk of collapse.
5. **Scenario 5**: During the procurement phase, a third-party supplier, without knowledge, introduces compromised firmware into pivotal components essential for satellite assembly. Despite undergoing stringent scrutiny and quality checks, these compromised components seamlessly infiltrate the manufacturing process due to the sophistication of the embedded malware. Following the satellite's launch, the embedded malicious firmware triggers surreptitious processes, granting unauthorized access to the satellite's intricate systems. This insidious breach compromises the very integrity of the satellite's functionalities, presenting an imminent threat of disruption to critical operations. The unauthorized access facilitated by the manipulated firmware poses severe risks to the satellite's functionality, potentially causing systemic failures and compromising its intended mission objectives.
6. **Scenario 6**: In a meticulously orchestrated cyber attack, threat actors execute a sophisticated manipulation of sensor data transmitted from the satellite to the ground station. Through the transmission of falsified data, they deceive ground operators into believing the authenticity of the compromised information. This deceitful manipulation prompts ground personnel to unknowingly execute erroneous commands, intending to align satellite components based on falsified information. However, this misalignment triggers subsequent functionality issues within the satellite system. The deceptive data manipulation severely impacts the satellite's operational precision, leading to potential malfunctions and disruptions in its functionality.

3.5. Mitigation and limitations

Onboard systems: Securing satellite units against cyber attacks demands a multi-faceted approach. Firstly, encryption stands as a fundamental safeguard (Falco, 2018b). Robust encryption protocols should be implemented to secure both stored and transmitted data, rendering it unreadable to unauthorized entities. This ensures the confidentiality of sensitive information even in the event of a breach. Authentication and access control mechanisms are crucial. Multi-factor authentication and stringent access controls limit interactions with the satellite's systems, ensuring that only authorized personnel can access and manipulate its functions, thereby reducing the risk of unauthorized entry (Pavur and Martinovic, 2022). Furthermore, ensuring the security of firmware and software is imperative. Regular updates and patches must be applied to mitigate vulnerabilities, while employing measures like code signing and integrity checks prevents unauthorized modifications or malware injections into the system. Continuous monitoring and response mechanisms are equally critical. A monitoring system that tracks the satellite's health and network traffic enables swift incident response, mitigating cyber threats promptly. Physical attacks on satellites such as debris and radiations are challenging to mitigate. However, it is important to consider that these solutions may introduce compatibility issues, increase weight, and drain power (Wright et al., 2005; Bergamasco et al., 2020; Hills et al., 2022). Additionally, there is a pressing need for more effective code analysis tools and formal verification processes, as the integration of third-party code into satellite software significantly increases the risk of software backdoors (Thangavel et al., 2022).

Communication Systems: To defend against communication vulnerabilities, several measures can be implemented. First and foremost, the use of strong encryption protocols is essential to ensure the confidentiality and integrity of communication channels (Tsai et al., 2023). Encryption mechanisms, such as Advanced Encryption Standard (AES) or Elliptic Curve Cryptography (ECC), can be employed to protect the data transmitted between satellites and ground stations (Vivero, 2013). However, the effectiveness of these encryption mechanisms may be threatened by quantum computers (Meraz and Vahala, 2020). Additionally, implementing robust authentication and authorization mechanisms, such as digital certificates and two-factor authentication, can help prevent unauthorized access and mitigate the risk of impersonation attacks. Furthermore, network monitoring and intrusion detection systems can be deployed to identify any suspicious activities or unauthorized access attempts in real-time (Mirchandani and Adhikari, 2020). These systems can detect anomalies in network traffic patterns and raise alerts when potential attacks are detected, allowing for timely response and mitigation measures (Kirshner, 2023; Marsili et al., 2023).

Ground Stations: Establishing a robust defense strategy for ground station cybersecurity demands a multi-layered approach encompassing technical, human, and administrative controls. Technically, deploying firewalls, intrusion detection systems, and antivirus software is pivotal in thwarting unauthorized access and malware infiltration. Regular software updates and patch management are crucial to counter emerging threats effectively. Human factors are equally crucial; stringent access management protocols fortified by robust authentication mechanisms mitigate unauthorized access attempts (Pearson, 2022). Augmenting physical security through surveillance systems, alarms, and access controls is critical. Administratively, ensuring operational resilience involves establishing redundancy and backup systems, enabling seamless operations during security breaches or equipment failures (Pearson, 2022). Regular security audits, vulnerability assessments, and penetration testing are integral for identifying and rectifying vulnerabilities (Pavur and Martinovic, 2019).

Ground station security challenges aren't exclusive to space systems; broader cybersecurity practices are applicable. Leveraging established cybersecurity frameworks, industry standards, and ongoing research significantly bolsters ground station defenses (Scholl, 2021). Addressing vulnerabilities in ground stations via proactive security approaches safeguards satellite communication systems' integrity, confidentiality, and availability.

These vulnerabilities stress the need for robust security measures in space information systems. Mitigating risks necessitates a multi-layered approach involving technological advancements, administrative controls, and comprehensive policy frameworks in addition to international cooperation (Li, 2023). Enhanced software/hardware security, regular vulnerability assessments, and patch management serve as crucial technical controls. Administrative controls, such as implementing stringent access control policies, conducting regular security training and awareness programs for personnel, establishing incident response protocols, and enforcing strict governance and compliance measures, play a pivotal role in fortifying cybersecurity. Additionally, robust policy frameworks outlining clear guidelines, regulations, and standards further contribute to the overall security posture of space systems. Prioritizing these technical, administrative, and policy-based cybersecurity measures ensures the safety, security, and sustainability of space infrastructure (Falco, 2018a; Santangelo, 2021). Integrating these layers—technical, administrative, and policy frameworks—within a comprehensive cybersecurity strategy empowers space agencies to effectively fortify their cyber resilience and safeguard critical space assets against evolving threats.

3.6. Comparative analysis: space cybersecurity vs. cybersecurity in other industries

Cybersecurity, a domain that permeates various industries, presents a spectrum of challenges and threat landscapes (Pedersen et al., 2022). A comparative analysis with space cybersecurity offers a lens to discern the unique hurdles the space sector grapples with and the potential lessons it can assimilate from other domains.

Banking and Financial Sector: The banking and financial sectors, alongside the space domain, remain prime targets for cyber adversaries. The financial sector's attractiveness stems from its vast monetary assets and extensive repositories of personal data (Vanini et al., 2023; Žunić et al., 2019). Conversely, the space sector's appeal lies in its strategic significance and pivotal infrastructure. Despite these commonalities, their response mechanisms diverge significantly.

In the financial realm, swift detection of unauthorized activities often enables prompt reversal, mitigating potential damages. However, in the space sector, a cyber onslaught on satellite systems can inflict irreversible harm, highlighting the critical disparity in response capabilities. This underscores the imperative for the space sector to adopt and adapt robust frameworks from the financial industry. Particularly, emulating the financial world's emphasis on multi-factor authentication, continuous monitoring, and swift incident response mechanisms becomes crucial to fortify the space domain's cyber resilience.

Healthcare Systems: In the rapidly advancing landscapes of healthcare and space technology, parallels in vulnerabilities have surfaced, shedding light on shared constraints that demand attention. Healthcare devices, such as implanted medical tools, face severe limitations owing to their compact form factors and limited power resources (Spanakis et al., 2020; Wazid et al., 2022; Kumar and Chand, 2020). These constraints often restrict the implementation of robust encryption protocols, creating vulnerabilities in ensuring secure system updates or enabling physicians to securely access patient data. Historical incidents have demonstrated the susceptibility of implanted devices, exemplifying the potential risks associated with compromised security measures. Similarly, space systems encounter comparable challenges due to the rigorous demands of space exploration. The need to minimize storage, computing, and power consumption in space-bound technology often results in compromises in security features. This compromise becomes evident in the vulnerability of space systems to cyberattacks or unauthorized access, mirroring the risks observed in healthcare devices. Breaches in healthcare not only jeopardize data integrity but also directly endanger human lives (Astillo et al., 2022; Wang et al., 2022a). In the same way, anomalies within space assets, particularly concerning navigation or communication satellites, hold the potential for widespread and potentially life-threatening repercussions. This underscores the critical imperative for the space industry to prioritize stringent lightweight security measures from the initial design phase, akin to the essential focus on securing systems in healthcare. Space technology can benefit from healthcare tech in cybersecurity by adopting encryption for secure communication, regular software updates, robust authentication measures, intrusion detection systems, and fostering collaboration for threat intelligence. Implementing these practices can bolster space systems' security, protect sensitive data, and mitigate potential cyber threats.

Energy and Utilities: Distributed architecture and redundancy have been pillars of resilience against non-malicious faults within energy systems. However, recent events have highlighted vulnerabilities in the face of targeted cyber attacks. For instance, the 2015 and 2016 cyberattacks on the Ukraine power grid exemplify how specific component compromise can lead to far-reaching outages, casting doubts on the presumed resilience of distributed systems in the face of malicious cyber threats (Li et al., 2022; Leao et al., 2022). Conversely, in space systems, a compromised satellite might lack an immediate substitute, highlighting a divergence in response capabilities. Interestingly, parallels emerge between the challenges faced by energy systems and those encoun-

tered in space infrastructure. Field devices in energy grids grapple with limitations akin to those in remote space systems: constrained computational power, difficulties in physical access due to remote locations, and infrequent updates to software and firmware (Presekal et al., 2023). These shared challenges indicate the vulnerabilities that adversaries can exploit, emphasizing the pressing need to address cybersecurity within energy systems comprehensively. Insights drawn from critical incidents serve as catalysts for change, compelling stakeholders to fortify infrastructure against evolving threats. This involves the deployment of advanced encryption protocols, the implementation of robust intrusion detection systems, and continuous monitoring to swiftly detect and neutralize potential cyber threats (Gao et al., 2022; Leao et al., 2022).

Manufacturing and Supply Chain:The complexities within the manufacturing and supply chain domains unveil multifaceted vulnerabilities (Velasco-Gallego and Lazakis, 2022; Truong et al., 2022). However, the aftermath of a breach delineates distinct implications between these sectors. In manufacturing, a tainted component could tarnish a specific product batch, whereas within the realm of space missions, the compromise of a solitary component holds the potential to catastrophically derail an entire mission. This stark contrast underscores the imperative for the space sector to adopt stringent supplier vetting processes, drawing insights and practices from the stringent standards observed in elite manufacturing protocols.

Unique Challenges in Space Cybersecurity: Space cybersecurity grapples with challenges unparalleled in other industries. The physical inaccessibility means that once a satellite is launched, any form of physical intervention becomes untenable. Coupled with their long operational lifespans, satellites might harbor outdated technology, becoming increasingly susceptible over time. The global purview of satellites complicates jurisdictional and legal nuances in the aftermath of a cyber incident. Furthermore, the dual-use nature of many satellites, catering to both civilian and military needs, makes them coveted targets for nation-state adversaries. The intricate interplay of ground stations, communication channels, and the satellite amplifies the vulnerability points.

While the space domain confronts distinct challenges, it stands to gain immensely from insights across industries. Embracing best practices, staying abreast of the evolving threat landscape, and championing international collaboration are paramount. As the space frontier becomes increasingly accessible and commercialized, a forward-thinking and comprehensive approach to cybersecurity is indispensable to protect the assets and services that are now pillars of contemporary existence.

4. Anomaly detection systems

4.1. Categories and types

Anomaly detection is a technique used to identify patterns or data points that deviate significantly from the normal behavior or expected patterns (Diro and Chilamkurti, 2018b). It plays a crucial role in various domains, including cybersecurity, fraud detection, system monitoring, and predictive maintenance. Anomaly types can be categorized as *point, contextual, collective, sequential, spatial, and collective contextual anomalies* according to their distinct characteristics and the nature of the data being analyzed (Diro et al., 2021a; He et al., 2022b).

Point anomaly detection focuses on detecting individual data points that exhibit significant deviations from the normal behavior of the data or network traffic (Cauteruccio et al., 2021). Statistical methods or machine learning algorithms analyze the characteristics of each data point to identify outliers or anomalies. This type of anomaly detection is useful in scenarios where individual instances carry important information, such as detecting fraudulent transactions or identifying faulty equipment. Contextual anomaly detection considers the context or relationships between data points when identifying anomalies (Nassif et al., 2021). It takes into account the expected behavior within a specific context and identifies anomalies based on how they deviate from this expected behavior. For example, in a time series network traffic, a data point may be considered an anomaly if it deviates significantly from the expected pattern based on historical context. Contextual anomaly detection is valuable in detecting anomalies that are context-dependent, such as detecting unusual patterns in network traffic or identifying abnormal behaviors in user activity. Collective anomaly detection, also known as group anomaly detection, focuses on identifying groups or subsets of data points that exhibit anomalous behavior as a whole, even if individual data points appear normal (Ahmed and Pathan, 2020). This type of anomaly detection is useful in scenarios where anomalies are not easily detectable at the individual level but become apparent when considering collective behavior. Applications include detecting coordinated attacks in cybersecurity or identifying unusual patterns in sensor networks. Sequential anomaly detection is employed in analyzing sequential or temporal data, where anomalies are detected based on their deviation from the expected sequence or pattern (Oh and Iyengar, 2019). This approach is commonly used in detecting fraud patterns in financial transactions, identifying network intrusions, or monitoring sensor data for anomalies. Spatial anomaly detection deals with identifying anomalies in spatial datasets, such as geographical data or image data (Song et al., 2021). Anomalies are detected by identifying data points or regions that significantly differ from the surrounding spatial context. This technique is useful in applications such as detecting abnormal hotspots in disease outbreaks or identifying unusual patterns in satellite imagery. Collective contextual anomaly detection combines both contextual and collective anomaly detection techniques (Dou et al., 2019). It aims to identify anomalies that occur in specific contexts or groups of data points, considering both the contextual information and the collective behavior of the data.

These different types of anomaly detection techniques provide a range of approaches to identify anomalies based on the specific characteristics and context of the data. By leveraging these techniques, organizations can gain valuable insights, improve decision-making processes, and detect abnormal behaviors or events that could pose potential risks or opportunities.

4.2. Techniques and approaches

There are several approaches to anomaly detection in traditional IT networks, including community-based methods, compression-based methods, decomposition-based methods, distance-based methods, and probabilistic model-based methods (Ranshous et al., 2015; Zhou and Tang, 2016).

4.2.1. Community-based methods

Community-based methods focus on identifying changes in the community structure of networks to detect anomalies (Zardi et al., 2022). These methods aim to find groups of nodes within the network that exhibit similar characteristics or behaviors. Anomalies are identified as nodes that do not belong to any of these communities. By analyzing the dynamics of these communities, community-based anomaly detection techniques can identify anomalies that deviate from the expected behavior within the network (Su et al., 2022). One common approach in community-based anomaly detection is modularity optimization. The modularity Q is computed by evaluating the difference between the observed number of edges within communities and the expected number of edges based on random connectivity. The modularity Q is given by:

$$Q = \frac{1}{2m} \sum_{i,j} \left(A_{ij} - \frac{k_i k_j}{2m} \right) \delta(c_i, c_j) \tag{1}$$

where, A_{ij} represents the connectivity or interaction between nodes i and j, k_i and k_j are the degrees of nodes i and j, m is the total connectivity strength in the network, c_i and c_j are the community assignments of nodes i and j, and $\delta(c_i, c_j)$ is a Kronecker delta function that is 1 if $c_i = c_j$ (i.e., the nodes belong to the same community) and 0 otherwise.

The optimization process aims to maximize the modularity Q by determining the most appropriate community assignments for the spacecraft or nodes. Anomalies are then identified as nodes that do not fit into any of the identified communities. By leveraging community-based anomaly detection, anomaly detection systems can identify abnormal behaviors, unexpected connections, or deviations from the expected patterns of spacecraft interactions. This can be crucial for detecting potential security threats, identifying malfunctions or failures in space systems, and ensuring the overall health and operational efficiency of networks.

Community-based anomaly detection methods leverage features such as node degree distribution, community structure, centrality measures, behavioral patterns, community evolution, cohesion, graph properties, temporal aspects, and content-based attributes to identify anomalies within network communities. These features are used in combination or separately, depending on the specific community-based anomaly detection method being employed, which could include techniques like community detection algorithms (e.g., modularity-based methods, spectral clustering, etc.) or graph-based anomaly detection algorithms. The choice of features often depends on the characteristics of the network being analyzed and the type of anomalies expected to be detected.

4.2.2. Compression-based methods

Compression-based methods can be employed to identify anomalies based on the extent to which a node or subgraph can be compressed without significant information loss (de la Torre-Abaitua et al., 2021; Lee et al., 2021). These methods leverage the notion that anomalies exhibit distinct characteristics that require more storage or encoding capacity compared to normal network components. The fundamental objective of compression-based methods is to detect anomalies by compressing the network data using a model and assessing the compression error. Anomalies are recognized as nodes or edges that cannot be adequately compressed by the model, resulting in a higher compression error relative to regular network elements. An example of a compression-based method used in anomaly detection is the Minimum Description Length (MDL) principle (Sabeti et al., 2021; Galbrun, 2022). According to the MDL principle, the optimal model minimizes the total encoding length of both the model itself and the data. Let M represent the model and D represent the network data. The MDL score is calculated as follows:

$$MDL = L(M) + L(D|M) \tag{2}$$

In this equation, L(M) denotes the length of the model M, and $L(D|M)$ represents the length of the network data D given the model M. By evaluating the MDL score, anomalies can be identified as nodes or edges with high MDL scores, indicating that their encoding requires additional resources and is less efficient compared to regular network components. Compression-based methods offer an alternative approach to anomaly detection by focusing on the compressibility of network data. By utilizing compression algorithms and evaluating the compression error, these methods can effectively detect anomalies that display unique or unexpected characteristics, deviating from the typical patterns observed in the network. This is particularly valuable in network anomaly detection such as SINs, where abnormal behavior, unexpected data patterns, or deviations from expected norms may indicate potential security threats, system malfunctions, or data anomalies that necessitate further investigation and attention.

Compression-based anomaly detection methods utilize features such as compression ratios, entropy measures, Kolmogorov complexity, model-based compression, and pattern frequency to detect anomalies by assessing the data's compressibility against expected norms. These methods typically rely on the intuition that anomalies or outliers possess characteristics that make them different from regular data in terms of compressibility, which can be captured by analyzing the compression properties of the data.

4.2.3. Decomposition-based methods

Decomposition-based methods are widely used in anomaly detection to identify anomalies by breaking down the network data into smaller components and detecting anomalies at the component level (Yu et al., 2018; Grabaskas and Si, 2017). These methods can capture the underlying structure of a network and identify anomalies based on deviations from expected patterns observed in the decomposed components. One commonly employed decomposition-based method in space anomaly detection is Singular Value Decomposition (SVD). SVD decomposes the adjacency matrix of the network into three matrices: U, S, and V^T. The matrices U and V contain orthogonal vectors, while the matrix S is a diagonal matrix of singular values. The objective is to find a low-rank approximation of the original adjacency matrix. Anomalies can then be identified as nodes or edges that exhibit significant reconstruction errors when compared to the low-rank approximation. This indicates that these components deviate from the expected patterns present in the network.

Decomposition-based and distance-based methods provide valuable approaches in anomaly detection, enabling the identification of anomalies by capturing the underlying structure of a network and measuring dissimilarities between network components (Bingqing et al., 2017). By leveraging these methods, anomalies can be effectively detected, helping to uncover unusual behaviors, security threats, or abnormal network phenomena that require further investigation and analysis.

Decomposition-based anomaly detection methods employ features such as residuals, principal components, independent components, wavelet coefficients, seasonal and trend components, matrix factors, dictionary elements, and latent space representations derived from decomposed data to quantify deviations and identify anomalies within the dataset. These features encapsulate different aspects of the data representations obtained through decomposition, allowing anomaly detection algorithms to quantify deviations from expected patterns or structures. The selection of features depends on the decomposition technique and the specific characteristics of the data under consideration.

4.2.4. Distance-based methods

Distance-based methods focus on measuring the distance or dissimilarity between nodes or edges in the network (Obied et al., 2023). These methods assess the dissimilarity of network components and identify anomalies based on larger distances or dissimilarities compared to normal network elements (Chatterjee and Ahmed, 2022). A notable example of a distance-based method used in space anomaly detection is the Mahalanobis distance method. The Mahalanobis distance D_{ij} between two nodes i and j is calculated as the square root of the difference between their feature vectors, taking into account the inverse of the covariance matrix S:

$$D_{ij} = \sqrt{(x_i - x_j)^T \cdot S^{-1} \cdot (x_i - x_j)} \tag{3}$$

Here, x_i and x_j represent the feature vectors of nodes i and j, respectively, and S denotes the covariance matrix of the feature vectors. Anomalies can be identified as nodes or edges that exhibit significant Mahalanobis distances, indicating substantial dissimilarity or distance compared to regular network components.

Distance-based anomaly detection methods commonly use numerical, categorical, binary, textual, geospatial, temporal, and image features to compute distances between data points and identify anomalies based on their deviation from normal patterns. The choice of features depends on the nature of the dataset and the specific problem being addressed.

4.2.5. Probabilistic model-based methods

Probabilistic model-based methods aim to detect anomalies by modeling the probability distribution of the network data and identifying anomalies as nodes or edges with low probability under the model. One example of a probabilistic model-based method is the Gaussian Mixture

Table 9
Comparison of Techniques for Space Anomaly Detection.

Method	Description	Advantage	Limitation
Community-based methods	Detect anomalies based on changes in the community structure of a network	Identify groups of nodes with similar characteristics	Assume anomalies deviate from community behavior
Compression-based methods	Detect anomalies based on the inability to compress a node or subgraph without significant loss	Effective in identifying anomalous patterns in network compression	Requires a suitable compression model and may not detect anomalies that are not compression-sensitive
Decomposition-based methods	Detects anomalies by decomposing the network data and identifying anomalies at the component level	Identifies anomalies based on large reconstruction errors	Requires a suitable decomposition method and may not detect anomalies that are not well-represented by components
Distance-based methods	Detect anomalies based on the distance or dissimilarity between nodes or edges	Suitable for identifying outliers or anomalies with distinct distances from normal instances	Require a proper distance or dissimilarity metric and may be sensitive to data scaling
Probabilistic model-based methods	Model the probability distribution of the network data and identifies anomalies with low probability	Capture the probabilistic nature of anomalies	Require assumptions about the underlying distribution and may struggle with complex anomaly patterns
Deep learning methods	Utilizes deep neural networks to learn complex patterns and relationships in the data	Can capture intricate spatial and temporal dependencies	Requires large amounts of labeled training data and computational resources

Model (GMM) method. GMM models the network data as a mixture of Gaussian distributions (Yu et al., 2023; Hundman et al., 2018). In anomaly detection, GMM is used to model the normal behavior of the network, and anomalies are detected based on the likelihood of the observed data under the learned model. The GMM can be represented by the following equation:

$$p(x) = \sum_{i=1}^{k} w_i \mathcal{N}(x|\mu_i, \Sigma_i)$$

where $p(x)$ is the probability density function of the GMM, k is the number of Gaussian components in the mixture, w_i is the weight of the i-th component, μ_i is the mean of the i-th component, Σ_i is the covariance matrix of the i-th component, and $\mathcal{N}(x|\mu_i, \Sigma_i)$ is the Gaussian distribution function with mean μ_i and covariance matrix Σ_i.

The parameters of the GMM can be learned from the observed data using the Expectation-Maximization (EM) algorithm. Once the GMM is learned, the log-likelihood of the observed data can be calculated as:

$$\ln p(X|\theta) = \sum_{n=1}^{N} \ln \left(\sum_{i=1}^{k} w_i \mathcal{N}(x_n|\mu_i, \Sigma_i) \right) \tag{4}$$

where X is the observed data, θ represents the parameters of the GMM, and N is the number of data points in X. Anomalies can be detected using the log-likelihood of the observed data under the learned model. Data points with low likelihood values are considered anomalies.

Probabilistic model-based methods provide an effective approach to anomaly detection as they enable the modeling of normal behavior in space information networks and the identification of anomalies based on the likelihood of observed data. These methods contribute to detecting abnormal network events, potential security breaches, or unexpected behaviors that warrant further investigation and analysis.

Probabilistic-based anomaly detection methods utilize statistical, temporal, spatial, frequency-based, correlation, behavioral, graph-based, and textual features to identify deviations from expected patterns within data. These features can be employed individually or in combination to create a feature space that is used by probabilistic-based anomaly detection algorithms to distinguish anomalies from normal data points. The choice of features often depends on the nature of the data and the specific problem domain.

The techniques are summarized in Table 9 in terms of their advantages and limitations for space anomaly detection.

4.3. Taxonomy

Anomaly detection can be classified into several taxonomies based on different criteria. These taxonomies can be used to identify the most suitable anomaly detection techniques for specific contexts based on their requirements and characteristics (Widhalm et al., 2020). Some of the commonly used taxonomies are data type, detection techniques, scope, application domain, data source, and temporal aspect.

Data type: Anomaly detection techniques encompass a wide array of methodologies, often classified based on the nature and structure of the data they analyze (Koroniotis et al., 2022). One fundamental classification revolves around the distinction between structured and unstructured data. Structured data, characterized by organized formats like databases or tables, often involves employing statistical methods such as Z-score analysis or Gaussian distribution models. Machine learning techniques like support vector machines (SVM) or decision trees, as well as clustering algorithms like k-means, are also commonly utilized for anomaly detection in structured data environments. Conversely, unstructured data—comprising formats such as text, images, or videos—poses unique challenges for anomaly detection. Natural Language Processing (NLP) techniques are leveraged for text-based data anomaly detection, while computer vision algorithms and deep learning models, such as autoencoders, play crucial roles in identifying anomalies within images or video datasets lacking a predefined structure.

Another significant classification pertains to time series data, where anomalies manifest in sequences of data points over time. Detecting anomalies in this type of data often involves methodologies like moving averages, change point detection, or the application of recurrent neural networks (RNNs) designed to capture temporal patterns and deviations. Furthermore, anomaly detection in streaming data, particularly in real-time or near real-time data streams, involves specialized techniques that continuously analyze incoming data to swiftly identify deviations from expected patterns. Graph-based anomaly detection techniques focus on identifying outliers or unusual patterns in network structures or interconnected data, offering insights into irregularities within complex relationships between entities. Additionally, hybrid approaches are increasingly common, combining multiple data types or leveraging various anomaly detection techniques simultaneously. These approaches integrate structured and unstructured data or employ a fusion of algorithms, enhancing detection accuracy and robustness by harnessing the strengths of different methodologies. Space systems use data such as telemetry, image, spectral, radio signals, and environmental (Zeng et al., 2022).

By categorizing anomaly detection techniques based on the type of data they operate on, practitioners can employ tailored methodologies and algorithms, ensuring effective anomaly detection across diverse data landscapes and application domains.

Detection technique: Detection techniques in anomaly detection encompass various methodologies tailored to different data types and structures (Luo et al., 2021b). One prominent approach involves the utilization of machine learning techniques, which aim to discern patterns within data and detect anomalies based on deviations from these es-

tablished patterns. Neural networks, including support vector machines (SVMs), decision trees, and ensemble methods like random forests are among the machine learning algorithms commonly employed for anomaly detection tasks. These algorithms learn from labeled or unlabeled data, distinguishing between normal and anomalous patterns.

Another approach involves deep learning, an advanced subset of machine learning that employs neural networks with multiple layers to automatically extract intricate features from data. Deep learning techniques, such as autoencoders, recurrent neural networks, and deep belief networks, excel in capturing complex patterns and are particularly effective in anomaly detection for unstructured data types like images, audio, and text (Xie et al., 2021). Signal processing techniques represent a specialized avenue for detecting anomalies in signal data, such as those generated by sensors. Fourier analysis, wavelet analysis, and other signal processing methods excel in identifying irregularities or unexpected changes within signal patterns, making them valuable tools for anomaly detection in time-series or sensor-generated data. Graph-based techniques represent data as interconnected nodes and edges, utilizing graph theory to uncover anomalies within network structures or interconnected datasets. Spectral clustering, community detection, and other graph-based anomaly detection methods excel in identifying outliers or unusual patterns within graph representations, offering insights into irregularities in relationships between entities.

By employing these diverse detection approaches—ranging from machine learning and deep learning techniques to signal processing methodologies and graph-based analyses—practitioners can address anomalies across a spectrum of data types and structures, ensuring comprehensive anomaly detection in various application domains.

Scope: Anomaly detection techniques are systematically classified according to the scope of the system under observation. This categorization strategy involves assessing the range or extent over which anomalies are being identified within a given dataset or system. The classification based on scope encompasses three primary categories: local scope, global scope, and hybrid scope (Koroniotis et al., 2022; Kon et al., 2022). Within the realm of local scope anomaly detection, the focus lies on pinpointing anomalies within specific data points that notably deviate from the general pattern exhibited by the rest of the dataset. Known as point anomalies, these outliers are detected using methods such as distance-based algorithms (e.g., k-nearest neighbors), density-based techniques (e.g., DBSCAN), or statistical models (e.g., Z-score). These approaches excel in identifying individual instances that stand out as irregularities within their local context.

Conversely, the global scope categorization involves identifying anomalies by considering the broader context or relationships within the entirety of the dataset or system. Contextual anomalies, detected at this level, are deviations from the overall behavior or patterns observed across the entire dataset. Techniques such as clustering algorithms (e.g., k-means), statistical modeling (e.g., Gaussian mixture models), or time-series analysis methods (e.g., ARIMA) are deployed to detect anomalies prevalent in the global scope. The hybrid scope classification integrates aspects of both local and global approaches by focusing on anomalies within subsets or groups of data instances. Collective anomalies, identified within this scope, involve abnormalities observed when examining clusters or associations of data instances rather than individual points or the entire dataset. Techniques such as graph-based algorithms (e.g., anomaly detection in social networks) or collaborative filtering methods (e.g., recommendation systems) excel in detecting collective anomalies by analyzing relationships or patterns within specific subsets or groups of data.

By classifying anomaly detection techniques based on scope, analysts and practitioners can tailor their approach to detect anomalies at varying levels of granularity within a system. This enables the selection of appropriate methods aligned with the specific analytical requirements, whether focused on pinpointing local outliers, assessing global patterns, or detecting anomalies within specific subsets or groups of data instances.

‘**Application domain**: Anomaly detection techniques exhibit diverse adaptations across various application domains, tailored to address specific challenges within each field. In the realm of cybersecurity, these methods play a pivotal role in identifying abnormal network behavior, intrusions, or suspicious activities within system logs and user actions. Anomaly-based intrusion detection systems, behavioral analysis models, and machine learning algorithms trained on network data serve as foundational tools in safeguarding digital environments. Finance and fraud detection rely extensively on anomaly detection to uncover irregularities in transactions, market behavior, and credit card usage patterns. Statistical methodologies, machine learning algorithms trained on transactional data, and sophisticated pattern recognition techniques form the backbone of fraud detection systems, ensuring timely identification of potentially fraudulent activities in financial transactions. In the healthcare sector, anomaly detection techniques analyze medical data, ranging from patient records to diagnostic images, to identify deviations indicating potential health issues. Machine learning models tailored for anomaly detection in time-series data, image analysis methods, and anomaly detection algorithms applied to vital signs monitoring contribute significantly to early disease diagnosis and patient care improvement.

Manufacturing and industry leverage anomaly detection techniques to maintain product quality and prevent equipment failures. Methods like statistical process control, sensor-based anomaly detection, and predictive maintenance algorithms enable the identification of faults or defects in products and machinery, facilitating enhanced operational efficiency. The Internet of Things (IoT) domain heavily relies on anomaly detection to ensure the security and reliability of interconnected devices and networks. Machine learning models, anomaly detection algorithms in streaming sensor data, and network traffic analysis techniques are pivotal in identifying irregularities or potential threats within IoT systems. Additionally, anomaly detection aids in natural disaster monitoring by analyzing environmental sensor data to detect unusual patterns indicative of impending disasters such as earthquakes, floods, or wildfires. Leveraging sensor data analysis, geospatial anomaly detection, and pattern recognition methods enables timely detection and mitigation of natural disasters, potentially saving lives and minimizing damage.

In network traffic analysis, anomaly detection techniques scrutinize network behavior, aiming to identify network intrusions or unusual traffic patterns signaling potential cyber threats. Statistical methods, machine learning algorithms, and deep learning approaches contribute to the early detection of anomalies within network traffic, ensuring robust cybersecurity measures in digital networks. These domain-specific applications of anomaly detection techniques highlight their versatility and crucial role in addressing distinct challenges across diverse fields. The application domain of anomaly detection in space information systems includes various areas such as Space Situational Awareness (SSA), Earth Observation, Remote Sensing, Navigation and Communication, Space Weather, and Spacecraft Operations (Falco, 2018a; Kennewell and Vo, 2013).

Data source: Sensor-generated data from IoT devices, industrial sensors, or health monitoring equipment serves as a fundamental source for anomaly detection (Nassar et al., 2015). These data streams contain crucial information about physical parameters or environmental conditions. Methods employed for anomaly detection in sensor data often involve statistical analysis, time-series modeling, machine learning algorithms, and signal processing techniques. These approaches aim to identify anomalies indicative of faults, unusual behavior, or irregular patterns in sensor readings, enabling timely intervention and maintenance. Network data, encompassing internet traffic, communication logs, or system records, forms the basis for anomaly detection in cybersecurity and network monitoring. Techniques applied to network traffic data aim to spot suspicious activities, intrusions, or deviations from normal network behavior. Utilizing machine learning models, statistical

analysis of traffic patterns, and behavioral analysis assists in detecting anomalies, enhancing security measures and threat detection.

Textual data derived from documents, social media, or customer feedback is essential in natural language processing (NLP) for anomaly detection. Methods in this domain involve sentiment analysis, topic modeling, and anomaly detection in language patterns. Detecting anomalies in language usage, shifts in sentiment, or irregular content utilizes machine learning and NLP methods, aiding in detecting unusual occurrences within textual information. Image and video data play significant roles in surveillance, medical imaging, and quality control. Techniques for anomaly detection in visual data involve computer vision algorithms, deep learning models, and image processing. These methods help identify anomalies like defects in products, unusual events in surveillance footage, or abnormalities in medical images, contributing to improved safety, quality, and diagnostics. Time series data from financial markets, weather monitoring, or energy consumption are analyzed for anomalies. Anomaly detection techniques in time series data encompass statistical analysis, time-series forecasting models, and machine learning algorithms. These methods aim to spot unexpected deviations, irregularities, or unusual patterns over time, facilitating proactive decision-making in various domains. In the context of anomaly detection in space information systems, data sources can include various sources of information such as satellite telemetry data, ground-based monitoring data, and data from other space-based sensors. The data can include information about various aspects of space operations such as spacecraft health, attitude, orbit, communications, and environmental factors such as radiation and space weather.

By classifying anomaly detection techniques according to the data source, tailored methodologies are applied across sensor data streams, network traffic, textual information, visual content, or time-dependent datasets, ensuring efficient anomaly detection in diverse application domains.

Temporal aspect: The temporal aspect plays a pivotal role in classifying anomaly detection techniques, delineating between real-time and offline detection methodologies (Li et al., 2013). Real-time detection involves continuous monitoring of data streams, allowing for immediate anomaly identification as data is generated. This approach is critical in time-sensitive domains like cybersecurity and IoT systems, where rapid responses to anomalies are imperative (Liu et al., 2022). Techniques employed in real-time detection, such as streaming algorithms and online machine learning models, enable swift anomaly detection, facilitating prompt action to mitigate potential risks.

In contrast, offline detection involves retrospectively analyzing historical data after the data collection period. This approach, unconstrained by real-time processing, focuses on comprehensive analysis using batch processing, traditional machine learning algorithms, and statistical methods. Offline detection is beneficial in fields like finance and healthcare, where a deep understanding of historical patterns and anomalies is essential for strategic decision-making and trend analysis.

The distinction between real-time and offline anomaly detection methodologies acknowledges the varied temporal needs across different applications. Real-time detection prioritizes immediate anomaly identification and response, ensuring swift action, while offline detection allows for thorough analysis of historical data, facilitating a deeper comprehension of long-term trends and anomalies. By aligning with the specific temporal requirements of each domain, these classification approaches assist practitioners in selecting suitable anomaly detection methods for their applications, optimizing response strategies and insights derived from the data. In space information systems, the temporal aspect is essential for detecting anomalies in the behavior of the spacecraft or the environment, such as changes in solar activity, radiation levels, or temperature. The detection of such anomalies can help prevent potential malfunctions or failures that could compromise the mission's success.

5. State of the art anomaly detection for space information networks

Anomaly detection within space information networks (SINs) is a critical area of research, given the increasing reliance on space systems for various applications. The realm of anomaly detection in space systems has witnessed a plethora of methodologies, ranging from traditional statistical approaches to advanced machine learning techniques. This section aims to provide an overview of the approaches employed for anomaly detection in SINs, and emphasizing their contributions, potential limitations, and practical implications. It is summarized in Table 10.

5.1. Overview

Machine learning algorithms are broadly categorized into supervised and unsupervised techniques for anomaly detection.

Supervised approaches require labeled data to train a model to classify data as anomalous or normal. These methods include support vector machines (SVM), decision trees, and neural networks. For example, SVM has been widely employed in the detection of anomalies in satellite imagery data (Malladi, 2017). Unsupervised approaches do not rely on labeled data and instead utilize clustering and outlier detection techniques to identify anomalous behavior. These methods include autoencoders, Gaussian mixture models (GMM), and isolation forests. For instance, Lang et al. (Lang et al., 2022) successfully applied GMM for the detection of anomalies in satellite attitude data. While machine learning-based methods have shown promising results in anomaly detection in space information systems, they also have several limitations (Diro and Chilamkurti, 2018a). Machine learning models such as deep neural networks are often considered black boxes because they lack interpretability. This can be particularly problematic in space information systems where understanding the root causes of anomalies is critical for system safety and reliability. Additionally, ML models may not generalize well to new datasets or scenarios outside of the training data. In space information systems, this can be problematic because the system behavior can vary greatly depending on the mission, hardware, and environmental factors (Di Francia et al., 2020).

Deep learning methods have gained prominence in the field of space anomaly detection due to their ability to capture complex patterns and relationships in space data (see Fig. 7). Two popular deep learning techniques utilized in this domain are Graph Convolutional Networks (GCNs) and Variational Autoencoders (VAEs). GCNs are specifically designed to handle graph-structured data, making them well-suited for analyzing space networks (Deng and Hooi, 2021). VAEs, on the other hand, are deep generative models that learn the underlying probability distribution of the space data (Niu et al., 2020; Ma et al., 2021). GCN neural networks learn representations of nodes by aggregating information from their neighboring nodes. The output of a GCN layer can be expressed as:

$$H^{(l+1)} = \sigma(\tilde{D}^{-\frac{1}{2}}\tilde{A}\tilde{D}^{-\frac{1}{2}}H^{(l)}W^{(l)}) \tag{5}$$

Here, $H^{(l)}$ denotes the node representation at layer l, $\tilde{A}$ represents the adjacency matrix of the space network with added self-loops, $\tilde{D}$ is the diagonal degree matrix of $\tilde{A}$, $W^{(l)}$ represents the weight matrix at layer l, and $\sigma(\cdot)$ is an activation function. Anomalies in the space network can be detected by analyzing the deviation of node representations from the learned normal behavior, as anomalies often exhibit distinct patterns that deviate from the expected space dynamics.

VAEs aim to capture a latent representation of the data that encapsulates the essential features and variations (Chen et al., 2021b). The encoder and decoder functions in VAEs are neural networks trained to model the encoder distribution $q_\phi(z|x)$ and decoder distribution $p_\theta(x|z)$, respectively. The latent variable z represents the compressed representation of the input space data. Anomalies can be detected by

Table 10
Comparison of space anomaly detection techniques.

Paper	Technique	Scalable?	Real-time?	Adaptable?	Explainable?	Multi-modal?	Adversarial free?
Fuertes et al. (2016)	SVM	No	No	No	No	No	No
Hundman et al. (2018)	LSTM	No	No	Yes	No	No	No
OMeara et al. (2016)	Outlier detection, supervised	No	No	No	No	No	No
Nalepa et al. (2022)	Various algorithms	No	No	No	No	No	No
Gunn et al. (2018)	LSTM	No	No	No	No	No	No
Shin et al. (2020)	Tensor-based, ML	No	No	No	No	No	No
He et al. (2022a)	Sparse feature extraction, ML	No	No	No	No	No	No
Wang et al. (2021)	Temporal Convolution Network (TCN)	No	No	No	No	No	No
Zhuo et al. (2021)	Statistical, ML, DL	No	No	No	No	No	No
Baireddy et al. (2021)	Transfer learning	No	No	No	No	No	No
Liu et al. (2023d)	LSTM +Transformer	No	No	No	No	No	No
Langfu et al. (2023)	K-Nearest Neighbor	No	No	No	No	No	No
Hou et al. (2023)	Transformer	No	No	No	No	No	No
Liu et al. (2023c)	Bayesian Model	No	No	No	Yes	No	No
Zhao et al. (2023)	Temporal Convolutional Autoencoder	No	No	No	Yes	No	No
Sadr et al. (2023)	Ensemble ML	No	No	No	No	Yes	No
Wang et al. (2023)	LSTM	No	No	No	No	Yes	No
Chen et al. (2021b)	Deep AutoEncoder	No	No	No	No	Yes	No
Chen et al. (2021a)	Bayesian LSTM	No	No	No	No	Yes	No
Xu et al. (2022)	LSTM	No	No	Yes	No	No	No
Guo et al. (2023)	Contrastive learning	No	No	No	No	No	No
Li et al. (2021b)	Statistical	No	No	Yes	Yes	No	No
Liu et al. (2017)	SVM	No	No	No	No	No	No
Soligo et al. (2021)	Gaussian Mixture	No	No	No	No	No	No
Wang et al. (2022b)	LSTM	No	No	No	No	No	No
Yuqing et al. (2016)	Statistical	No	No	No	No	No	No
Li et al. (2021a)	SVM	No	No	No	No	No	No
Jiang et al. (2019)	Statistical	No	No	No	No	No	No
Zeng et al. (2022)	Attentio-LSTM	No	No	No	Yes	No	No
Zeng et al. (2022)	LSTM	Yes	No	No	No	No	No
Li et al. (2020)	Bayesian Model	No	No	No	No	No	No
Liu et al. (2021)	Statistical	No	No	No	No	No	No
Jin et al. (2021)	Convolutional Autoencoders	No	No	No	No	No	No
Pan et al. (2020)	BI-LSTM	No	No	No	No	No	No
Abdelghafar et al. (2019)	Extreme Learning Machine (ELM)	No	No	No	No	No	No

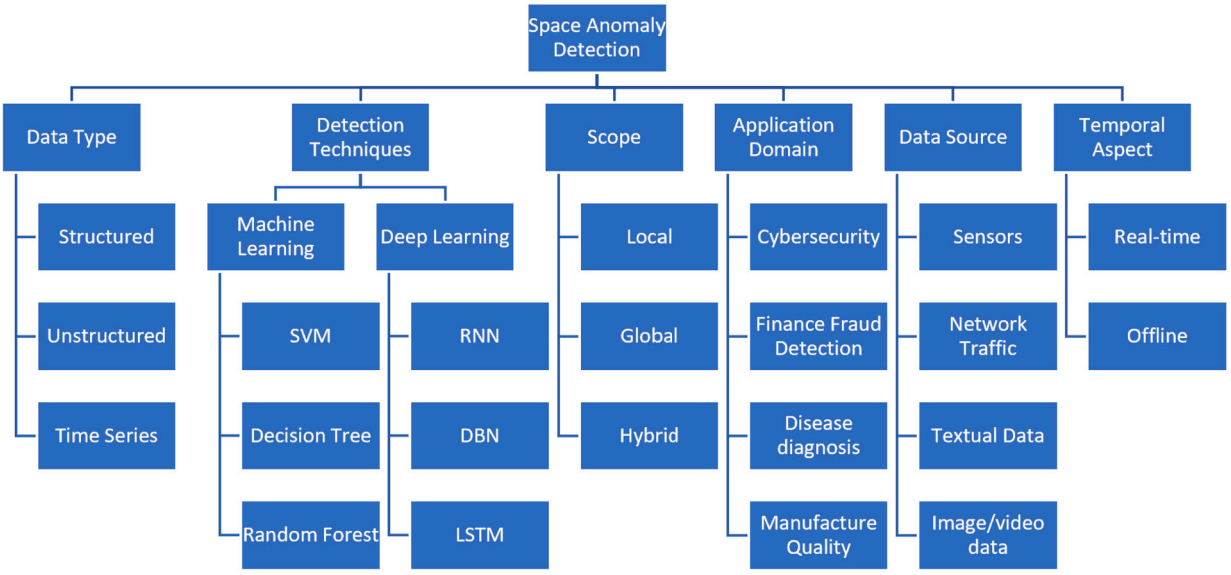

Fig. 7. Space anomaly detection taxonomy.

evaluating the likelihood of the observed data under the learned probabilistic model, as anomalous instances tend to have lower likelihoods compared to normal instances. The application of deep learning methods for space anomaly detection is an active area of research. Further advancements are necessary to address the unique challenges of space data, such as high-dimensional and time-varying characteristics. Additionally, the development of innovative deep learning architectures and training strategies specifically tailored to space anomaly detection will contribute to more accurate and efficient detection of anomalies in space networks.

Deep learning-based methods have shown great potential in anomaly detection. However, their lack of interpretability is a significant limitation. Explainable AI techniques can be used to provide interpretable explanations for the detected anomalies (Liu et al., 2021). For example, attention mechanisms can be used to highlight the regions of an image or video that contribute to anomaly detection. Similarly, saliency maps and gradient-based methods can be used to highlight the most important features in the data that contribute to anomaly detection. By providing interpretable explanations for the detected anomalies, these methods can help operators to understand the root causes of anomalies and take appropriate actions (Xie et al., 2021; Tritscher et al., 2023).

5.2. Machine learning for anomaly detection in SINS

Several studies delve into spacecraft anomaly detection methodologies and systems. Fuertes et al. (Fuertes et al., 2016) explore Support Vector Machines' (SVM) utility in spacecraft health monitoring, highlighting its rapid anomaly identification but urging further scalability exploration. OMeara et al. (2016) present Athmos, an Automated Telemetry Health Monitoring System, leveraging outlier detection and machine learning but possibly limited in identifying subtle or evolving anomalies. In contrast, Shin et al. (2020) propose ITAD (Integrative Tensor-based Anomaly Detection), utilizing tensor-based data representation, yet acknowledging its varied performance across applications. He et al. (2022a) propose a sparse feature-based approach addressing false positives, while Langfu et al. (2023) introduce a balanced time series dataset method using DTW oversampling and Fast-DTW, exhibiting enhanced anomaly detection. Additionally, Liu et al. (2023c) showcase AFWBM, an adjustable feature-weighted Bayesian model, excelling in dual-working and multiworking anomaly detection. Sadr et al. (2023) focus on proactive spacecraft issue diagnosis using Multivariate Variance-based Genetic Ensemble (MVVGE). Furthermore, Guo et al. (2023) introduce CLPNM-AD, employing contrastive learning for spacecraft anomaly detection. The study by Li et al. (2021a) presents a fault monitoring method emphasizing resource efficiency and adaptability. Additionally, Liu et al. (2017) focus on fragment anomalies in spacecraft health management, while Soligo et al. (2021) propose automated anomaly detection in satellite telemetry. Other researches such as Yuqing et al. (2016) and Li et al. (2021a) detail anomaly detection in satellite power subsystems and momentum wheel voltage telemetry data, respectively. Moreover, Jiang et al. (2019) explore pseudo-periods in satellite telemetry data for anomaly detection. Li et al. (2020) propose a dynamic anomaly detection method for satellite power supply telemetry parameters, and Liu et al. (2023a) introduce a combined detection method for Signal-in-Space (SIS) anomalies in the BeiDou Navigation Satellite System (BDS).

5.3. Deep learning approaches for anomaly detection in SINS

The paper by Hundman et al. (2018) introduces Long Short-Term Memory (LSTM) neural networks and nonparametric dynamic thresholding for spacecraft anomaly detection, demonstrating improved accuracy over traditional methods but highlighting LSTM's interpretability challenges. Gunn et al. (2018) propose an LSTM-based method for satellite communication anomaly detection, aiming to enhance detection accuracy while stressing the need for further investigation into generalizing findings. Wang et al. (2021) propose a Temporal Convolution Network (TCN) for spacecraft telemetry anomaly detection, showcasing its superiority over LSTM-based solutions. Baireddy et al. (2021) leverage transfer learning and pre-trained convolutional neural networks (CNN) for spacecraft anomaly detection across various anomaly types. In their study (Hou et al., 2023), an Improved Transformer model coupled with a self-supervised framework demonstrates enhanced performance for satellite telemetry anomaly detection. PEAR method introduced in Liu et al. (2023d) showcases improved satellite anomaly detection by addressing temporal patterns' oversight in telemetry data. The DRTCAE model proposed in Zhao et al. (2023) using Advanced Dilated Causal Convolutional blocks exhibits superior performance over traditional methods in anomaly detection. Wang et al. (2023) present the MFCA-LSTM model, enhancing telemetry sequence prediction and anomaly detection for satellite operation reliability. Chen et al. (2021b) propose the VAE/BLGAN model for early anomaly detection in satellite telemetry data, exhibiting superior learning ability. They introduce a Bayesian LSTM model for anomaly detection in satellite telemetry in Chen et al. (2021a), showing enhanced detection capabilities on imbalanced datasets. Xu et al. (2022) utilize an LSTM-AE model for anomaly detection in satellite telemetry, demonstrating its effectiveness through real-world case studies. Wang et al. (2022b) introduce a DDMN-based approach for point anomaly detection in satellite telemetry, showcasing its performance and deployment for real-time monitoring. Zeng et al. (2022) propose CN-FA-LSTM, a framework for satellite anomaly detection, emphasizing interpretability and superior performance. Han et al. (2023) introduce DDMN for anomaly detection in satellite telemetry, aiming to minimize satellite failures and ensure orbital health. Lastly, Jin et al. (2021) explore autoencoders for identifying anomalies in satellite power subsystems, demonstrating their enhanced detection capacity.

5.4. Analysis

Traditional machine learning techniques employed for anomaly detection within space information networks encounter multifaceted challenges. These methods often grapple with the complexity inherent in capturing deep representations within the datasets. The intricate relationships and complex correlations present in high-dimensional telemetry data pose difficulties for these conventional techniques. Consequently, their ability to discern nuanced anomalies, especially those emerging gradually or evolving over time, remains constrained. Moreover, traditional approaches frequently rely on predefined feature engineering, which can be inadequate in encapsulating the diverse and intricate patterns intrinsic to space telemetry data, hampering their efficacy in anomaly detection. In addition, the dynamic and ever-evolving nature of space information networks further exacerbates the limitations of traditional methods. Anomalies within such networks may manifest as subtle deviations that evolve gradually over time, presenting a significant challenge for traditional anomaly detection techniques that may struggle to adapt to these dynamic environments. Furthermore, the computational inefficiencies faced by these methods when dealing with large volumes of streaming telemetry data in real-time can lead to scalability issues, potentially causing delays in anomaly identification and compromising the timeliness of response mechanisms. Another notable challenge is the handling of imbalanced data distributions, where anomalies occur infrequently compared to normal operational data within telemetry datasets. Traditional techniques often face difficulties in effectively addressing this class imbalance, leading to biased anomaly detection. Moreover, the robustness of these methods is often compromised when faced with noisy or incomplete telemetry data, making them susceptible to higher false positives or missing genuine anomalies due to data irregularities. Additionally, capturing complex temporal and spatial dependencies prevalent in telemetry data poses a significant challenge for these techniques, limiting their capability

to detect anomalies demonstrating such dependencies. However, with the advent of deep learning, newer methods like deep autoencoders, Generative Adversarial Networks (GANs), and Recurrent Neural Networks (RNNs) have also been employed for anomaly detection in SINS, producing significant improvements over traditional machine learning approaches.

Lessons Learned: Deep learning techniques have emerged as powerful tools for anomaly detection within space information networks, offering several advantages in handling complex telemetry data (Wu et al., 2020). These methods, such as neural networks like Long Short-Term Memory (LSTM) and Convolutional Neural Networks (CNNs), excel in recognizing intricate patterns and correlations present in high-dimensional telemetry datasets. Their ability to detect subtle anomalies that might elude traditional methods is a significant benefit, especially in complex space networks where anomalous behavior might not follow explicit patterns. Another advantage lies in the autonomous feature learning capability of deep learning models. They can extract relevant features directly from raw telemetry data, eliminating the need for manual feature engineering. This adaptability is particularly advantageous in space networks where data patterns might change over time due to evolving mission requirements or environmental conditions. However, these benefits come with certain limitations. One of the major drawbacks of deep learning models, especially complex architectures, is their lack of interpretability. They are often perceived as black boxes, making it challenging to understand and interpret the reasoning behind their anomaly detection decisions. In critical space operations, this lack of interpretability could hinder trust and comprehension. Furthermore, deep learning algorithms typically require large volumes of labeled data for effective training. Acquiring labeled anomaly data in space information networks can be challenging, as anomalies might be rare, diverse, or costly to obtain. Additionally, the computational demands of deep learning models can pose challenges in space systems with limited computational resources, potentially impacting real-time anomaly detection capabilities. Another critical concern is the vulnerability of deep learning models to adversarial attacks. Maliciously crafted input data can mislead the model, leading to incorrect anomaly predictions. In security-sensitive space systems, this susceptibility to attacks could pose a significant threat to the reliability and security of the network. Therefore, while deep learning holds promise for anomaly detection in space information networks, addressing interpretability issues, data requirements, computational demands, and vulnerability to attacks is crucial. Overcoming these limitations will be imperative in harnessing the full potential of deep learning while ensuring the reliability, security, and interpretability of anomaly detection systems in space. On the other hand, traditional machine learning and threshold-based methods, despite their limitations, can provide valuable insights, especially when computational resources are limited. As space systems continue to evolve, a hybrid approach that combines the strengths of various techniques might emerge as the optimal solution for anomaly detection. It's worth noting that deep learning-based methods like LSTMs, TCNs, and CNNs depend on compression and community-based approaches.

The trajectory of research in anomaly detection within space information networks (SINs) is emblematic of the broader evolution of computational methodologies. Historically, the reliance on threshold-based techniques, while foundational, has revealed a series of inherent limitations. These techniques, while rudimentary and straightforward, often suffer from a lack of adaptability. Their deterministic nature, which predicates anomaly detection on predefined thresholds, is ill-suited to the multifaceted and dynamic nature of space systems. The high incidence of false alarms is not merely an operational inconvenience but can have profound implications for mission-critical operations, potentially jeopardizing both equipment and data integrity. The ascendancy of deep learning, particularly LSTM architectures, in this domain is a testament to the quest for greater accuracy and adaptability. LSTMs, with their capacity to model sequential data, offer a more nuanced approach to anomaly detection. Their ability to "remember" and "learn" from historical data makes them particularly adept at identifying patterns that might elude more traditional methods. The evolution from threshold-based techniques to deep learning in SIN anomaly detection is reflective of a broader shift from deterministic to probabilistic and adaptive methodologies in computational research. This transition, while promising, is not without its challenges. It underscores the perennial tension between simplicity and accuracy, between interpretability and effectiveness. Their black-box nature, computational intensity, and the need for extensive labeled data for training are significant hurdles. Furthermore, the dynamic nature of SINs, characterized by evolving nodes and connections, presents a unique challenge. The current research landscape, while increasingly sophisticated, seems to be playing catch-up with the rapid advancements and changes in space network configurations. As these networks evolve, so too do the nature and type of anomalies. This fluidity demands anomaly detection systems that are not just sophisticated but also inherently adaptable.

6. Dynamic space anomaly detection system: architecture, and methods

This section introduces a novel dynamic space anomaly detection system and proposes its taxonomy, architecture, and methods.

6.1. Overview

Dynamic networks have become increasingly important for modeling complex interactions in real-world information systems (Zhu et al., 2020). These networks have the capability to capture rich temporal and spatial information for each edge, enabling a deeper understanding of system evolution and dynamics. Their significance is evident across various domains, including e-commerce, social networks, and computer networks, as they provide informative features and insights into these systems. Unlike static networks, dynamic networks accurately represent real-world systems by capturing the changing nature of relationships and interactions between objects. In the context of space information networks, which manage and control the flow of information among satellites, spacecraft, and ground stations, the dynamic nature of these networks is paramount (Zhu et al., 2020). Space anomaly detection (SAD) can leverage anomaly detection methods employed in dynamic networks, such as social and transport networks. Given the changing conditions in space, including object movement and variations in the communication environment, robust and adaptable anomaly detection methods are crucial for space networks. Real-time detection of anomalies is essential to ensure network reliability, and efficiency, and to prevent potential harm to space assets. By drawing on the advancements in anomaly detection methods for dynamic networks, space anomaly detection can benefit from the ability to capture evolving anomalies and adapt to changing conditions. This approach allows for the development of effective anomaly detection techniques that can address the unique challenges and requirements of space information networks, ensuring the safety and reliability of space systems.

Anomalies in dynamic networks can be caused by various factors, including cyber-attacks, network failures, or changes in the underlying structure of the network. Anomaly detection in dynamic networks is the task of identifying unusual behavior or events in time-varying networks from large-scale data (Viswanathan and Pecharich, 2016). The detection is challenging due to the large and complex nature of such networks, as well as the need to process and analyze data in real-time. In dynamic networks, anomalous edge detection focuses on identifying abnormal relationships between nodes in the network. This type of anomaly detection takes into account not only the networked data but also the temporal evolution of the edges over time, providing a more comprehensive view of the network dynamics. This is important for identifying potential security threats, fraud, or other anomalies in the network. Graph embedding methods have become a powerful tool for handling large-scale complex networks, providing effective solutions for

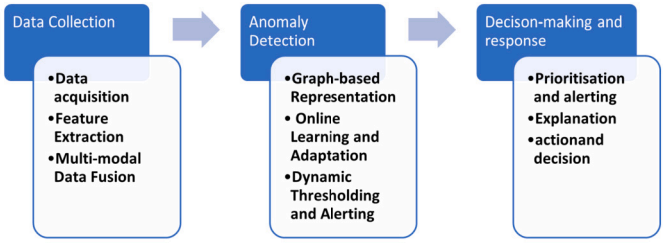

Fig. 8. A Possible Architecture of space anomaly Detection.

learning low-dimensional vector representations that preserve network structure and properties.

6.2. Architecture

In space information networks, where communication links can experience high latency, limited bandwidth, and disruption due to environmental factors, traditional anomaly detection schemes may not be suitable (Diro, 2021). A distributed anomaly detection scheme with multiple sensors throughout the network can be adopted for space anomaly detection, which can detect local anomalies and communicate with each other to detect global anomalies (Bosman et al., 2017; Diro et al., 2021b). Such a scheme is suitable for space information networks because it can detect anomalies in real-time and reduce the network's dependence on a central control unit, making the network more robust against disruptions. Additionally, distributed anomaly detection schemes can use machine learning algorithms that can adapt to changing network conditions, making them more effective at detecting anomalies in the dynamic and complex environment of space information networks.

A space anomaly detection system typically consists of three main components, as shown in Fig. 8.

- *Data collection*: This component is responsible for collecting and processing data from various sources such as satellites, ground-based sensors, and other spacecraft. It is responsible for extracting relevant features from the raw data collected by the sensors. Advanced feature extraction techniques, such as wavelet transforms, Fourier analysis, or time-frequency analysis, can be employed to capture intricate patterns and characteristics of the data. These extracted features provide more informative representations for anomaly detection algorithms. As the system operates with distributed sensors, it is crucial to fuse the data collected from multiple sensors to gain a comprehensive understanding of the network behavior. Advanced data fusion techniques, such as Kalman filtering, Bayesian inference, or Dempster-Shafer theory, can be employed to integrate and combine the information from various sensors, improving the accuracy and robustness of anomaly detection.
- *Anomaly detection*: This component uses various algorithms and techniques to detect anomalies in the preprocessed data. Space information networks can often be represented as graphs, where nodes represent entities (e.g., spacecraft, ground-based sensors) and edges represent their relationships or interactions. By utilizing graph-based representations, advanced graph mining techniques, such as graph clustering, graph motif detection, or graph embedding, can be applied to capture complex network structures and detect anomalies that manifest as structural deviations or unusual patterns in the graph. In dynamic space environments, the system should be capable of adapting to changing conditions and evolving anomalies. Online learning algorithms, such as online clustering or incremental learning methods, can be integrated into the system to continuously update the anomaly detection models as new data becomes available. This enables the system to adapt to new patterns and anomalies in real-time. An advanced dynamic space anomaly detection system should incorporate dynamic thresholding mechanisms to differentiate between normal variations and anomalous behavior. Thresholds can be dynamically adjusted based on contextual information, historical data, or statistical methods to adapt to varying network conditions. Once an anomaly is detected, the system should generate alerts or notifications with appropriate severity levels, providing actionable information for decision-making and response.
- *Decision-making and response*: Once an anomaly is detected, this component is responsible for making a decision on the severity of the anomaly and triggering an appropriate response. To facilitate effective monitoring and decision-making, the system can include a user-friendly interface that allows human operators to interact with the anomaly detection system. The interface can provide visualizations of the network status, real-time anomaly alerts, and tools for in-depth analysis and investigation. Human expertise can be leveraged to validate and interpret anomalies, refine anomaly detection models, and make informed decisions based on the detected anomalies.

6.3. Methods

An anomaly detection system in dynamic networks is a system designed to detect and identify abnormal or unusual patterns in network data. This system can be used to monitor and analyze satellite data, data from space-based sensors, and other space-related data sets. An anomaly detection system in dynamic space networks is a critical tool for ensuring the safety and security of space-related operations. It allows for the identification of potential threats and enables organizations to take appropriate action to mitigate those risks (Nizam et al., 2022). There are several approaches to anomaly detection in dynamic networks that can be adopted for space anomaly detection, including streaming and graph methods.

6.3.1. Streaming methods

Streaming anomaly detection is well-suited for space anomaly detection in dynamic space information networks (SINs) due to its ability to enable real-time monitoring and detection of anomalies (Rettig et al., 2019). SINs are complex systems that are prone to various anomalies, such as system failures, data corruption, cyber-attacks, and environmental factors. Streaming anomaly detection techniques can quickly and accurately identify these anomalies, ensuring the safety and reliability of space missions. Moreover, streaming methods can help mitigate the issues of false positives and false negatives commonly encountered in traditional anomaly detection approaches that rely on static models or thresholds. By continuously updating the model and adapting to changes in network behavior, streaming methods provide more accurate and reliable results. This adaptability is crucial in SINs, where the consequences of false alarms or missed detections can be severe. Additionally, streaming anomaly detection can be combined with other techniques, such as machine learning or statistical methods, to enhance the accuracy and effectiveness of the detection process. This hybrid approach leverages the strengths of different techniques, resulting in a more comprehensive and robust solution (Degirmenci and Karal, 2022).

One specific streaming method suited to space anomaly detection is the Concept Drift-based Streaming Anomaly Detection scheme (Zhu et al., 2020). This scheme is designed to detect changes in the normal behavior of a network over time, which is particularly useful in dynamic networks like SINs where behaviors can rapidly and unpredictably change. The approach involves using statistical or machine learning algorithms to model the normal behavior of the network. As the network behavior evolves, the model is updated to reflect these changes. When a significant change is detected, such as concept drift, an alarm is raised to alert network administrators of a potential anomaly. The key advantage of this approach is its ability to adapt to changes in network behavior, making it suitable for networks subject to frequent

changes. By promptly detecting concept drift, network administrators can identify and respond to potential anomalies, thereby preventing or minimizing the impact of cyber-attacks or security incidents. Concept drift-based anomaly detection offers several benefits for space anomaly detection, including early anomaly detection, real-time adaptation, improved resilience, scalability, and automation.

In Concept Drift-based Streaming Anomaly Detection, algorithms are employed to detect changes in the distribution of network behavior and adjust the model accordingly to maintain accurate anomaly detection in dynamic SINs. A commonly used equation for concept drift detection is the Cusum test (Kurt et al., 2020):

$$C_t = \max(0, C_{t-1} + (Y_t - \mu)) \tag{6}$$

Here, C_t represents the cumulative sum at time t, Y_t is the new data, and μ is the expected mean. If the cumulative sum exceeds a threshold, it indicates the presence of concept drift. Once concept drift is detected, the model is adapted to reflect the new distribution of network behavior. The model updating equation is often represented as:

$$\begin{aligned} &\text{if } \Delta < \epsilon, W_t = W_{t-1} + \eta \cdot (Y_t - \hat{Y}t) \cdot X_t \\ &\text{if } \Delta \geq \epsilon, W_t = Wt - 1 \end{aligned} \tag{7}$$

In this equation, W_t represents the updated weight, η is the learning rate, Y_t is the actual value, $\hat{Y}_t$ is the predicted value, X_t is the input data, Δ is the difference between the current and previous weight, and ϵ is the threshold for detecting concept drift.

Another streaming method, Multi-Modal Streaming Anomaly Detection (Yoo et al., 2021), integrates multiple sources of data, such as network logs can be used to detect anomalies in dynamic SINs. The approach combines information from diverse sources to improve anomaly detection accuracy. It can be represented as:

$$\hat{Y}t = W_1 \cdot X1_t + W_2 \cdot X_{2_t} + \ldots + W_n \cdot X_{n_t} \tag{8}$$

Here, $\hat{Y}t$ is the predicted value, and $X1_t, X_{2_t}, \ldots, X_{n_t}$ represent the input data from different sources. $W_1, W_2, \ldots, W_n$ are the weights assigned to each source, reflecting their relative importance in the anomaly detection process.

The updated model, incorporating the multi-modal data, is then used to detect anomalies in the real-time stream of data. One commonly used equation for this purpose is the Mahalanobis distance (Leys et al., 2018):

$$d = (x - \mu)^T \Sigma^{-1} (x - \mu) \tag{9}$$

In this equation, d represents the Mahalanobis distance, x is the data point, μ is the mean, Σ is the covariance matrix, and Σ^{-1} is the inverse of the covariance matrix. Data points with a high Mahalanobis distance are considered outliers or anomalies.

By leveraging streaming methods like Concept Drift-based Streaming Anomaly Detection and Multi-Modal Streaming Anomaly Detection, space anomaly detection systems can adapt to the dynamic nature of SINs, detect changes in network behavior, and identify anomalies in real-time. These techniques provide valuable insights for ensuring the safety, reliability, and security of space missions by enabling early detection, reducing false positives and false negatives, and enhancing the overall accuracy and effectiveness of the anomaly detection process.

6.3.2. Graph methods

Anomaly scores can be computed based on the structural properties of the graph (Zheng et al., 2019; Ma et al., 2021). In this case, graph centrality measures, such as degree centrality, closeness centrality, or betweenness centrality, can be used to identify nodes that deviate significantly from the expected patterns (Akoglu et al., 2015). The mathematical representation for computing anomaly scores using centrality measures can be written as:

$$s_i = f(\text{Centrality}(G, v_i)) \tag{10}$$

where s_i is the anomaly score for node v_i, $\text{Centrality}(G, v_i)$ represents the centrality measure for node v_i in graph G, and $f(\cdot)$ is a mapping function that transforms the centrality measure into the anomaly score.

Graph clustering techniques can also identify groups or clusters of nodes that exhibit similar behavior, and anomalies can be detected as nodes that do not conform to any cluster (Studiawan et al., 2017). Spectral clustering is a popular graph clustering algorithm, which utilizes the eigenvalues and eigenvectors of the graph Laplacian matrix (Guo and Liu, 2023). The mathematical representation for spectral clustering can be given as:

$$\arg, \min C \sum i, j A_{ij} \cdot |X_i - X_j|^2 \tag{11}$$

where C represents the set of clusters, A is the adjacency matrix of the graph, X_i and X_j are feature vectors of nodes v_i and v_j, and $|\cdot|$ denotes a distance metric.

Anomaly propagation techniques leverage the concept that anomalies tend to spread their influence to neighboring nodes in the graph. The Label Propagation algorithm is commonly used to assign anomaly labels to nodes based on the labels of their neighbors. The mathematical representation for anomaly propagation can be written as:

$$s_i = \sum_{v_j \in N(v_i)} w_{ij} \cdot s_j \tag{12}$$

where s_i is the anomaly score for node v_i, $N(v_i)$ represents the set of neighboring nodes of v_i, w_{ij} denotes the weight between nodes v_i and v_j, and s_j represents the anomaly score of node v_j.

Attention mechanisms are techniques used in machine learning and artificial intelligence to focus on specific parts of input data (Zhou et al., 2022). This approach can be applied to space cybersecurity to improve the ability to detect and respond to potential threats in space networks. Attention mechanisms can be used in various ways, including feature identification and prioritizing alerts. Graph Attention Networks (GATs) are a type of neural network architecture used for processing graph-structured data. They use attention mechanisms to weigh the importance of different nodes in the graph, enabling them to focus on the most relevant information. GATs can be employed for tasks such as node classification, link prediction, and graph generation. In the context of space anomaly detection, GATs can be used to analyze data from satellites or telescopes, such as images or sensor readings. By treating the data as a graph, with nodes representing objects or regions of interest and edges representing relationships between them, GATs can identify patterns or anomalies indicating the presence of unknown objects or phenomena (Zhao et al., 2020). For anomaly detection in space networks, GATs can be combined with a reconstruction error-based approach. The equations for the GAT-based anomaly detection process using attention weight computation are as follows:

$$\alpha_{ij} = \text{LeakyReLU}\left(a^T [W_x x_i || W_h h_j]\right) \tag{13}$$

Here, x_i represents node i's feature vector, h_j is the hidden representation of the neighboring node j, $||$ denotes the concatenation operator, and a, W_x, and W_h are learnable parameters. The node representation update is computed as:

$$h_i = \sum(\alpha_{ij} \cdot h_j) \tag{14}$$

In this equation, α_{ij} denotes the attention weight between node i and node j, and h_j is the hidden representation of the neighboring node j. The temporal attention weight is computed as:

$$\beta_{it} = \text{LeakyReLU}\left(b^T [W_h h_i || W_t t_i]\right) \tag{15}$$

Here, t_i represents node i's timestamp, and b and W_t are learnable parameters. The temporal node representation update is performed as:

$$h_{it} = \sum(\beta_{it} \cdot h_{i(t-1)}) \tag{16}$$

In this equation, β_{it} denotes the temporal attention weight between node i at time t and node i at time $t-1$, and $h_{i(t-1)}$ is the hidden representation of node i at time $t-1$. The reconstruction error is computed as:

$$L = ||h_{i(T)} - h_{i(0)}||^2 \tag{17}$$

Here, L represents the reconstruction error, $h_{i(T)}$ is the updated node representation of node i at the final time step T, $h_{i(0)}$ is the initial node representation, and $||\cdot||^2$ denotes the L2 loss function. The anomaly score is computed as:

$$s_i = \exp\left(-\frac{L_i}{T}\right) \tag{18}$$

Here, s_i represents the anomaly score for node i, L_i is the reconstruction error for node i, and T is the temperature parameter controlling the sensitivity of the anomaly score. Nodes with high anomaly scores are considered anomalies in the dynamic network.

These approaches, including Temporal Graph Convolutional Networks (TGCNs) and Graph Attention Networks (GATs), can provide effective methods for detecting anomalies in space networks. TGCNs capture both spatial and temporal dependencies in the dynamic graph structure, while GATs leverage attention mechanisms to focus on relevant information in the graph. By utilizing these techniques, space anomaly detection systems can effectively monitor and identify unusual changes or deviations from the normal pattern, enabling timely detection and response to potential threats in space networks.

6.3.3. Graph streams methods

A graph network stream is denoted as $\mathbb{G} = {G^t}_{t=1}^T$, where T is the time length of the graph $\mathbb{G}$, and $G^t = (V^t, \epsilon^t)$ represents a graph snapshot at a given time t, with V^t being the set of nodes and ϵ^t being the set of edges. In this context, a relationship exists between nodes v_i^t and v_j^t at time t if there exists an edge $e_{i,j}^t = (v_i^t, v_j^t) \in \epsilon^t$, where $v_i^t, v_j^t \in V^t$. The main objective of anomaly detection in dynamic graph networks is to compute the abnormality of an edge, known as the anomaly score, by employing a learnable function $f(e_{i,j}^t)$, where a high score indicates a high probability of an anomalous edge (Liu et al., 2021). Dynamic network anomaly detection systems involve monitoring changes in the graph structure over time and identifying any unusual deviations from the normal pattern.

One approach to dynamic network anomaly detection suitable for SINs is the utilization of temporal graph convolutional networks (TGCN) (Luo et al., 2021a), which extend graph convolutional networks (GCNs) to handle time-varying graphs. TGCNs are deep learning models designed to process data with both temporal and graph-based dependencies. They are specifically tailored for scenarios where the data can be represented as a graph, and the structure of the graph evolves over time. TGCNs employ graph convolutions to perform message passing between nodes in a graph, and they use recurrent neural networks (RNNs) to model the temporal dependencies of the data. By combining these two components, TGCNs learn both the spatial and temporal features of the data. The TGCN-based dynamic network anomaly detection process can be defined as follows:

$$h_i^l = \text{ReLU}\left(\sum_j (A_{ij} \cdot h_j^{l-1} \cdot W_l) + \sum_t (S_{it} \cdot h_i^{l-1}(t) \cdot V_l)\right) \tag{19}$$

Here, h_i^l represents the hidden representation of node i in layer l. A is the adjacency matrix of the graph, h_j^{l-1} is the hidden representation of neighboring node j in layer $l-1$, W_l is a learnable weight matrix for layer l, S is the temporal adjacency matrix representing the temporal relationships between nodes, $h_i^{l-1}(t)$ is the hidden representation of node i in layer $l-1$ at time t, V_l is a learnable weight matrix for the temporal relationships in layer l, and ReLU represents the activation function. The reconstruction error L is computed as:

$$L = ||h_i^L(T) - h_i^0||^2 \tag{20}$$

In this equation, $h_i^L(T)$ is the hidden representation of node i in the final TGCN layer at the final time step T, h_i^0 is the initial node feature representation, and $||\cdot||^2$ denotes the L2 loss function. The anomaly score s_i can be computed as:

$$s_i = \exp\left(-\frac{L_i}{T}\right) \tag{21}$$

Here, s_i represents the anomaly score for node i, L_i is the reconstruction error for node i, and T is the temperature parameter that controls the sensitivity of the anomaly score. Nodes with high anomaly scores are considered anomalies in the dynamic network.

The strengths of the stream and graph-based techniques can be leveraged to achieve more accurate and comprehensive results in space anomaly detection. Let $\mathbb{G} = {G^t}_{t=1}^T$ represent the stream of graph snapshots over time, where T is the time length of the graph stream. Each $G^t = (V^t, \epsilon^t)$ represents a graph snapshot at time t, with V^t denoting the set of nodes and ϵ^t denoting the set of edges.

First, we apply streaming methods to detect anomalies in the dynamic network stream. This involves continuously updating the model and adapting to changes in the network behavior. We can use a concept drift-based streaming anomaly detection scheme represented as:

$$C_t = \max(0, C_{t-1} + (Y_t - \mu)) \tag{22}$$

where C_t is the cumulative sum, Y_t is the new data, and μ is the expected mean. If the cumulative sum exceeds a threshold, it indicates a concept drift and potentially an anomaly.

Next, we incorporate graph methods to capture the structural dependencies and temporal aspects of the dynamic graph network. We employ Temporal Graph Convolutional Networks (TGCNs) to handle time-varying graphs. The node representation update in TGCN can be expressed as:

$$h_i^l = \text{ReLU}\left(\sum_j (A_{ij} \cdot h_j^{l-1} \cdot W_l) + \sum_t (S_{it} \cdot h_i^{l-1}(t) \cdot V_l)\right) \tag{23}$$

where h_i^l is the hidden representation of node i in layer l, A is the adjacency matrix of the graph, h_j^{l-1} is the hidden representation of neighboring node j in layer $l-1$, W_l is the learnable weight matrix for layer l, S is the temporal adjacency matrix representing the temporal relationships between nodes, $h_i^{l-1}(t)$ is the hidden representation of node i in layer $l-1$ at time t, and V_l is the learnable weight matrix for the temporal relationships in layer l.

To compute the reconstruction error for anomaly detection, we compare the final hidden node representation $h_i^L(T)$ at the final time step T with the initial node feature representation h_i^0:

$$L = ||h_i^L(T) - h_i^0||^2 \tag{24}$$

Finally, the anomaly score can be calculated as:

$$s_i = \exp\left(-\frac{L_i}{T}\right) \tag{25}$$

where s_i is the anomaly score for node i, L_i is the reconstruction error for node i, and T is the temperature parameter controlling the sensitivity of the anomaly score.

By combining streaming methods for real-time monitoring and detection of anomalies with graph methods that capture structural and temporal dependencies, this proposed approach provides a more robust and accurate solution for space anomaly detection in complex and dynamic space information networks. Our proposed anomaly detection model endeavors to identify anomalies within space information networks originating from a spectrum of sources, encompassing not only cybersecurity threats but also anomalies arising from diverse causes. This collaborative approach spans nodes both in space and ground stations, promoting a holistic view of network integrity. While ground

stations adhere steadfastly to established cybersecurity practices, our model's scope extends beyond the conventional purview, aiming to bolster the overall reliability of satellite systems by adeptly detecting and mitigating anomalies from various sources. By fostering collaboration between nodes in space and ground stations, our anomaly detection model promotes a synergistic network defense strategy. This comprehensive approach aims to fortify the resilience of space information networks, enabling proactive responses to diverse anomalies, thereby safeguarding the integrity and functionality of satellite systems.

Real world application: Anomaly detection within dynamic Graph Streams Methods relies on crucial features specific to satellite systems. Monitoring connectivity alterations, latency, packet loss, and traffic patterns in Network Features identifies irregularities in data transmission rates and communication structures among satellites. Payload Features scrutinize payload modifications and content, ensuring data integrity within the constellation. Command and Control Features monitor command sequences, access attempts, and unauthorized operations across satellite networks. Telemetry Features observe shifts in received data from satellite constellations. Additional Depth Features analyze energy consumption, frequency spectrum, hardware health, and geospatial anomalies.

In a constellation, the detection of anomalies relies on the continuous analysis of constellation-specific features evolving over time. For instance, fluctuations in inter-satellite connectivity patterns over time serve as crucial indicators. Monitoring these changes facilitates the detection of shifting communication links and evolving data transmission behavior among satellites. Similarly, the continual analysis of orbital parameters and satellite positions offers insights into the dynamic nature of satellite orbits and positions, allowing the identification of irregularities as they evolve over time. Cross-link communication metrics, such as signal strength and latency, undergo temporal variations within a constellation. By employing these time-varying metrics, anomalies or irregular communication behaviors among constellation satellites can be identified. Synchronization protocols and signals continuously evolve among satellites, and highlighting these temporal shifts helps detect inconsistencies or deviations in synchronization signals within the constellation. Furthermore, the analysis of multi-satellite coordination protocols over time reveals temporal deviations or irregularities in coordinated activities across satellites. Observing changes in propulsion activities and maneuvers among satellites over time aids in the detection of unexpected or unauthorized propulsion operations within the constellation. Additionally, tracking alterations in constellation layout, ground contact durations, and potential interferences with external satellite networks, with an emphasis on their temporal evolution, helps identify irregularities or anomalies as they dynamically change over time. The focus on the time-evolving nature of constellation-specific features enables graph stream methods to effectively capture, monitor, and detect anomalies within satellite constellations. By continuously analyzing these evolving features, anomalies, irregular behaviors, or deviations from expected patterns can be identified, ensuring comprehensive and adaptive anomaly detection capabilities within dynamic and evolving space environments.

7. Challenges and future directions

Dynamic space networks, encompassing intricate satellite constellations, advanced interplanetary communication systems, and sophisticated space-based sensors, underpin the contemporary advancements in space operations (Falco, 2019). As these networks undergo expansion and evolution, they introduce multifaceted challenges, underscoring the imperative for pioneering solutions in anomaly detection (Popova, 2023).

7.1. Scalability and complexity

The accelerated expansion of space networks, exemplified by ambitious undertakings such as Starlink and OneWeb, precipitates an unparalleled influx of data. Conventional anomaly detection methodologies, including SVM and PCA, while proficient in more constrained environments, may encounter limitations in the face of this voluminous and intricate data (Abdelghafar et al., 2019; Ferguson et al., 2015). Emerging deep learning paradigms, notably CNNs and RNNs, present promising avenues. For instance, CNNs, renowned for their image processing capabilities, can be adeptly deployed to scrutinize satellite imagery, discerning anomalies such as unanticipated celestial object trajectories or aberrant thermal signatures (Chen et al., 2021c; Dromard et al., 2016).

The exigency for real-time processing is paramount. Envision a satellite constellation dedicated to real-time climate surveillance on Earth. Any latency in data assimilation and processing could potentially overlook pivotal climatic anomalies. By harnessing edge computing directly on satellites and synergizing it with cloud capabilities, one can ensure prompt data processing and anomaly detection (Ahmad and Purdy, 2016).

7.2. Data challenges

Owing to the infrequency of anomalies in space operations, procuring labeled data emerges as a significant challenge (Nalepa et al., 2022; Habeeb et al., 2019; Yang et al., 2022). Technological advancements proffer potential solutions. Simulations, meticulously crafted to emulate scenarios such as satellite component malfunctions or communication impediments, can furnish invaluable data for model training. Additionally, the domain of transfer learning offers intriguing prospects. A model, initially trained for terrestrial communication networks, might, with appropriate refinements, be repurposed for deep-space communication systems (Tan et al., 2018; Baireddy et al., 2021). Furthermore, the advent of GANs facilitates the synthesis of anomaly data, augmenting training datasets and enhancing model robustness (Habeeb et al., 2019).

7.3. Model challenges

The inherent dynamism of space networks often culminates in the phenomenon of concept drift, wherein the network's behavior undergoes temporal transformations (Korycki and Krawczyk, 2021; Sun et al., 2020). This necessitates the development of models that are not merely static but possess the capability to adapt and evolve. Online learning paradigms, characterized by their continuous learning capabilities, are apt for such dynamic environments. Moreover, reinforcement learning, with its iterative feedback-driven approach, emerges as a potent tool in these mutable terrains (Sanchez et al., 2020; Korycki and Krawczyk, 2022; Kurakin et al., 2016).

Space networks are not impervious to adversarial attacks, wherein data is insidiously manipulated with malevolent intent (Mumcu et al., 2022). In such contexts, adversarial training methodologies, which train models on a blend of genuine and perturbed data, can serve as a robust defense mechanism. For instance, in scenarios where a space network is subjected to deliberate signal interference, models fortified through adversarial training can discern and counteract these disruptions (Korycki and Krawczyk, 2022).

7.4. Explainability

With the burgeoning complexity of algorithms, elucidating their decision-making processes becomes an academic challenge (Huang and Wu, 2022; Poore et al., 2016; Soize, 2017). This complexity often evokes the metaphor of a black box, wherein the inputs and outputs are discernible, but the internal logic remains enigmatic. However, innovative tools such as SHAP and LIME offer a semblance of clarity (Antwarg

et al., 2021). For instance, if a model identifies a satellite's behavior as anomalous due to a distinct thermal signature, tools like SHAP can elucidate the significance of this thermal feature in the decision-making process, offering invaluable insights to researchers and practitioners (Antwarg et al., 2021).

Summary: Dynamic space anomaly detection is pivotal in safeguarding the integrity of space missions and networks (Guo et al., 2021). The ability to promptly and accurately pinpoint anomalies is instrumental in averting potential system disruptions, mitigating associated risks, and upholding the robustness of space operations. Yet, the evolving nature of space networks introduces multifaceted challenges.

One of the primary challenges is scalability. As space networks burgeon, the sheer volume and complexity of data demand algorithms that can scale efficiently. Traditional methods might falter under the weight of this data deluge, emphasizing the need for innovative solutions that can process data in real-time (Abdelghafar et al., 2019). Another significant hurdle is the scarcity of labeled data, which is vital for training robust anomaly detection models. This paucity underscores the importance of simulations and transfer learning techniques, which can bridge the data gap and enhance model training (Nalepa et al., 2022). Furthermore, the dynamic nature of space networks means they are susceptible to concept drift, where previously established norms evolve over time. This fluidity necessitates the development of adaptive models that can learn and adjust to these changing patterns (Korycki and Krawczyk, 2021). Compounding these challenges are adversarial attacks, where malevolent entities deliberately manipulate data to induce or hide anomalies. Ensuring the robustness of anomaly detection systems against such attacks is paramount, calling for techniques like adversarial training and data sanitization (Mumcu et al., 2022).

To navigate these challenges, an interdisciplinary approach is essential. Collaborative efforts between domain experts, such as astronomers and data scientists, can yield innovative solutions that meld domain-specific knowledge with cutting-edge algorithmic approaches (Shen et al., 2019). Additionally, integrating anomaly detection with other network analysis techniques and fostering human-machine collaboration can offer a holistic understanding of space networks. Hence, the quest for effective dynamic space anomaly detection is ongoing. As technology and research progress, so will the methods and techniques employed in this domain. The end goal remains consistent: to ensure the security, resilience, and success of space operations amidst ever-evolving challenges and threats.

8. Conclusion

The space industry's rapid growth brings both opportunities and challenges. This article focuses on the challenges posed by the increasing cyberthreat landscape in space information networks (SINs) and the need for proactive measures and innovative solutions to ensure the security of space operations. It provides a comprehensive exploration of the historical context and evolution of cyber threats in SINs, identifies vulnerabilities and threats in space networks, and presents a detailed taxonomy of anomaly detection in SINs. The survey further examines previous studies and highlights key hurdles, including scalability, real-time detection, limited labeled data, concept drift, and adversarial attacks targeting space. To address these challenges, the article proposes the use of graph stream techniques, which can effectively capture the intricate temporal and structural dependencies in space networks and enhance anomaly detection accuracy. The article concludes by offering future directions and recommendations as a roadmap to guide researchers and practitioners in advancing the field. By embracing these recommendations and leveraging innovative approaches, the space industry can strengthen its anomaly detection capabilities, ensure the security of space networks, and facilitate continued exploration and utilization of space resources.

CRediT authorship contribution statement

Abebe Diro: Conceptualization, Methodology, Writing – original draft, Writing – review & editing. **Shahriar Kaisar:** Writing – original draft, Writing – review & editing, Visualization. **Athanasios V. Vasilakos:** Writing – original draft, Writing – review & editing. **Adnan Anwar:** Writing – original draft, Writing – review & editing. **Araz Nasirian:** Writing – original draft, Writing – review & editing, Visualization. **Gaddisa Olani:** Writing – original draft, Writing – review & editing.

Declaration of competing interest

The authors declare no conflict of interest.

Data availability

No data was used for the research described in the article.

References

Abdelghafar, S., Darwish, A., Hassanien, A.E., Yahia, M., Zaghrout, A., 2019. Anomaly detection of satellite telemetry based on optimized extreme learning machine. J. Space Saf. Eng. 6, 291–298.

Abdulmonem, M.H., Ismail, A.K., Mostafa, H., 2021. Design and implementation of authenticated encryption co-processors for satellite hardware security. In: 2021 International Conference on Microelectronics (ICM). IEEE, pp. 40–44.

Abeshu, A., Chilamkurti, N., 2018. Deep learning: the frontier for distributed attack detection in fog-to-things computing. IEEE Commun. Mag. 56, 169–175.

Abuabed, Z., Alsadeh, A., Taweel, A., 2023. Stride threat model-based framework for assessing the vulnerabilities of modern vehicles. Comput. Secur. 133, 103391.

Ahmad, I., Suomalainen, J., Porambage, P., Gurtov, A., Huusko, J., Höyhtyä, M., 2022. Security of satellite-terrestrial communications: challenges and potential solutions. IEEE Access 10, 96038–96052.

Ahmad, S., Purdy, S., 2016. Real-time anomaly detection for streaming analytics. ArXiv preprint. arXiv:1607.02480.

Ahmed, M., Pathan, A.-S.K., 2020. Deep learning for collective anomaly detection. Int. J. Comput. Sci. Eng. 21, 137–145.

Akoglu, L., Tong, H., Koutra, D., 2015. Graph based anomaly detection and description: a survey. Data Min. Knowl. Discov. 29, 626–688.

Al-Rodhan, N., 2020. Cyber security and space security. Space Rev. 26.

Antwarg, L., Miller, R.M., Shapira, B., Rokach, L., 2021. Explaining anomalies detected by autoencoders using Shapley additive explanations. Expert Syst. Appl. 186, 115736.

Astillo, P.V., Duguma, D.G., Park, H., Kim, J., Kim, B., You, I., 2022. Federated intelligence of anomaly detection agent in iotmd-enabled diabetes management control system. Future Gener. Comput. Syst. 128, 395–405.

Atmaca, U.I., Maple, C., Epiphaniou, G., et al., 2022. Challenges in threat modelling of new space systems: a teleoperation use-case. Adv. Space Res. 70, 2208–2226.

Bailey, B., 2020. Establishing Space Cybersecurity Policy, Standards, and Risk Management Practices. Aerospace Corporation El Segundo, CA.

Baireddy, S., Desai, S.R., Mathieson, J.L., Foster, R.H., Chan, M.W., Comer, M.L., Delp, E.J., 2021. Spacecraft time-series anomaly detection using transfer learning. In: Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition, pp. 1951–1960.

Barbaroux, P., 2016. The metamorphosis of the world space economy: investigating global trends and national differences among major space nations' market structure. J. Innov. Econ. Manag., 9–35.

Baselt, G., Strohmeier, M., Pavur, J., Lenders, V., Martinovic, I., 2022. Security and privacy issues of satellite communication in the avlatlon domain. In: 2022 14th International Conference on Cyber Conflict: Keep Moving!(CyCon), volume 700. IEEE, pp. 285–307.

Baylon, C., 2014. Challenges at the intersection of cyber security and space security. Int. Secur.

Beazley, M., 2020. Making space for Australia. J. Proc. R. Soc. N. S. W. 153, 39–41.

Bergamasco, F., Cassar, R., Popova, R., 2020. Cybersecurity: Key Legal Considerations for the Aviation and Space Sectors. Kluwer Law International BV.

Bingqing, F., Shaolin, H., Chuan, L., Yangfan, M., 2017. Anomaly detection of spacecraft attitude control system based on principal component analysis. In: 2017 29th Chinese Control and Decision Conference (CCDC), pp. 1220–1225.

Blount, P., 2017. Satellites are just things on the Internet of things. Air Space Law 42.

Blount, P., 2023. Space cybersecurity and us law. In: Routledge Handbook of Commercial Space Law. Routledge, pp. 503–514.

Book, G., 2006. Security Threats Against Space Missions. CCSDS Secretariat, Washington, DC, USA.

Borgia, S., Topputob, F., Zaneroc, S., 2023. Hack: a holistic modeling approach for cubesat cyberattacks. In: Aerospace Science and Engineering: III Aerospace PhD-Days 33, p. 281.

Boschetti, N., Gordon, N., Sigholm, J., Falco, G., 2022a. Commercial space risk framework assessing the satellite ground station security landscape for nato in the Arctic and high North. In: MILCOM 2022-2022 IEEE Military Communications Conference (MILCOM). IEEE, pp. 679–686.

Boschetti, N., Gordon, N.G., Falco, G., 2022b. Space cybersecurity lessons learned from the viasat cyberattack. In: ASCEND 2022, p. 4380.

Bosman, H.H., Iacca, G., Tejada, A., Wörtche, H.J., Liotta, A., 2017. Spatial anomaly detection in sensor networks using neighborhood information. Inf. Fusion 33, 41–56.

Brukardt, R., 2022. How will the space economy change the world? https://www.mckinsey.com/industries/aerospace-and-defense/our-insights/how-will-the-space-economy-change-the-world. (Accessed 20 June 2023) [Online].

Calabrese, M., 2023. Space Oddity: Space Cybersecurity Lessons from a Simulated OPS-SAT Attack. Master's thesis. NTNU.

Caudill, H., 2020. Big risks in small satellites: the need for secure infrastructure as a service. In: ASCEND 2020, p. 4017.

Cauteruccio, F., Cinelli, L., Corradini, E., Terracina, G., Ursino, D., Virgili, L., Savaglio, C., Liotta, A., Fortino, G., 2021. A framework for anomaly detection and classification in multiple iot scenarios. Future Gener. Comput. Syst. 114, 322–335.

Chatterjee, A., Ahmed, B.S., 2022. Iot anomaly detection methods and applications: a survey. Int. Things 19, 100568.

Chen, J., Pi, D., Wu, Z., Zhao, X., Pan, Y., Zhang, Q., 2021a. Imbalanced satellite telemetry data anomaly detection model based on bayesian lstm. Acta Astronaut. 180, 232–242.

Chen, J., Zhao, X., Pi, D., 2021b. A deep auto-encoder satellite anomaly advance warning framework. Aircr. Eng. Aerosp. Technol. 93, 1085–1096.

Chen, S., Jin, G., Ma, X., 2021c. Detection and analysis of real-time anomalies in large-scale complex system. Measurement 184, 109929.

Chowdhury, P., Paul, S.K., Kaisar, S., Moktadir, M.A., 2021. Covid-19 pandemic related supply chain studies: a systematic review. Transp. Res., Part E, Logist. Transp. Rev. 148, 102271.

Cunningham, D.E., Palavincini Jr, G., Romero-Mariona, J., 2016. Towards effective cybersecurity for modular, open architecture satellite systems. In: Small Satellite Conference.

Cyr, B., Long, Y., Sugawara, T., Fu, K., 2023. Position paper: space system threat models must account for satellite sensor spoofing. In: SpaceSec23.

David Wright, L.G., Gronlund, L., 2005. The physics of space security. https://aerospace.csis.org/wp-content/uploads/2019/06/physics-space-security.pdf. (Accessed 20 June 2023) [Online].

de la Torre-Abaitua, G., Lago-Fernández, L.F., Arroyo, D., 2021. A compression-based method for detecting anomalies in textual data. Entropy 23, 618.

Degirmenci, A., Karal, O., 2022. Efficient density and cluster based incremental outlier detection in data streams. Inf. Sci. 607, 901–920.

Deng, A., Hooi, B., 2021. Graph neural network-based anomaly detection in multivariate time series. Proc. AAAI Conf. Artif. Intell. 35, 4027–4035.

Di Francia, G., De Vito, S., Formisano, F., Del Giudice, A., Aurigemma, R., Fortezza, R., Savino, R., Moriello, S.S.L., 2020. Heterogeneous sensor network for micro-satellite anomaly detection and event recording. In: 2020 IEEE 7th International Workshop on Metrology for AeroSpace (MetroAeroSpace). IEEE, pp. 211–216.

Diro, A., 2021. Collaborative and integrated edge security architecture. In: Secure Edge Computing. CRC Press, pp. 21–39.

Diro, A., Chilamkurti, N., 2018a. Leveraging lstm networks for attack detection in fog-to-things communications. IEEE Commun. Mag. 56, 124–130.

Diro, A., Chilamkurti, N., Nguyen, V.-D., Heyne, W., 2021a. A comprehensive study of anomaly detection schemes in iot networks using machine learning algorithms. Sensors 21, 8320.

Diro, A., Mahmood, A., Chilamkurti, N., 2021b. Collaborative intrusion detection schemes in fog-to-things computing. In: Fog/Edge Computing for Security, Privacy, and Applications, pp. 93–119.

Diro, A.A., Chilamkurti, N., 2018b. Distributed attack detection scheme using deep learning approach for Internet of things. Future Gener. Comput. Syst. 82, 761–768.

Dou, S., Yang, K., Poor, H.V., 2019. Pc 2 a: predicting collective contextual anomalies via lstm with deep generative model. IEEE Int. Things J. 6, 9645–9655.

Dromard, J., Roudiere, G., Owezarski, P., 2016. Online and scalable unsupervised network anomaly detection method. IEEE Trans. Netw. Serv. Manag. 14, 34–47.

Elmarady, A.A., Rahouma, K., 2021. Studying cybersecurity in civil aviation, including developing and applying aviation cybersecurity risk assessment. IEEE Access 9, 143997–144016.

Eriksson, J., Giacomello, G., 2022. Cyberspace in space: fragmentation, vulnerability, and uncertainty. In: Cyber Security Politics. Routledge, pp. 95–108.

Falco, G., 2018a. The vacuum of space cyber security. In: 2018 AIAA SPACE and Astronautics Forum and Exposition, p. 5275.

Falco, G., 2018b. Job one for space force: space asset cybersecurity. Belfer Center, Harvard Kennedy School, Belfer Center for Science and International Affairs, Harvard Kennedy School 79.

Falco, G., 2019. Cybersecurity principles for space systems. J. Aerosp. Inform. Syst. 16, 61–70.

Falco, G., 2020. When satellites attack: satellite-to-satellite cyber attack, defense and resilience. In: ASCEND 2020, p. 4014.

Falco, G., Boschetti, N., 2021. A security risk taxonomy for commercial space missions. In: ASCEND 2021, p. 4241.

Falco, G., Viswanathan, A., Santangelo, A., 2021. Cubesat security attack tree analysis. In: 2021 IEEE 8th International Conference on Space Mission Challenges for Information Technology (SMC-IT). IEEE, pp. 68–76.

Falco, G., Korth, L., Custer, P., Schofield, R.N., Pocock, C., 2023. How to scrub a launch: spaceport cybersecurity. In: 2023 IEEE 9th International Conference on Space Mission Challenges for Information Technology (SMC-IT). IEEE, pp. 56–67.

Ferguson, D.C., Worden, S.P., Hastings, D.E., 2015. The space weather threat to situational awareness, communications, and positioning systems. IEEE Trans. Plasma Sci. 43, 3086–3098.

Fick, A.S. Nathaniel, Miscik, Jami, Goldstein, G.M., 2022. Confronting reality in cyberspace. https://www.cfr.org/task-force-report/confronting-reality-in-cyberspace/download/pdf/2022-07/CFR_TFR80_Cyberspace_Full_SinglePages_06212022_Final.pdf. (Accessed 20 June 2023) [Online].

Forester, C., 2015. Russia "eavesdropping" on satellite operations, Inside Satellite TV.

Fritz, J., 2013. Satellite hacking: a guide for the perplexed. Cult. Mandala 10, 5906.

Fuertes, S., Picart, G., Tourneret, J.-Y., Chaari, L., Ferrari, A., Richard, C., 2016. Improving spacecraft health monitoring with automatic anomaly detection techniques. In: 14th International Conference on Space Operations, p. 2430.

Galbrun, E., 2022. The minimum description length principle for pattern mining: a survey. Data Min. Knowl. Discov. 36, 1679–1727.

Gao, H.-X., Kuenzel, S., Zhang, X.-Y., 2022. A hybrid ConvLSTM-based anomaly detection approach for combating energy theft. IEEE Trans. Instrum. Meas. 71, 1–10.

Gorman, S., Dreazen, Y.J., Cole, A., 2009. Insurgents hack us drones. Wall St. J. 17.

Grabaskas, N., Si, D., 2017. Anomaly detection from Kepler satellite time-series data. In: Machine Learning and Data Mining in Pattern Recognition: 13th International Conference, MLDM 2017, New York, NY, USA, July 15-20, 2017, Proceedings 13. Springer, pp. 220–232.

Gunn, L., Smet, P., Arbon, E., McDonnell, M.D., 2018. Anomaly detection in satellite communications systems using lstm networks. In: 2018 Military Communications and Information Systems Conference (MilCIS). IEEE, pp. 1–6.

Guo, G., Hu, T., Zhou, T., Li, H., Liu, Y., 2023. Contrastive learning with prototype-based negative mixing for satellite telemetry anomaly detection. Sensors 23, 4723.

Guo, H., Li, J., Liu, J., Tian, N., Kato, N., 2021. A survey on space-air-ground-sea integrated network security in 6g. IEEE Commun. Surv. Tutor. 24, 53–87.

Guo, Y., Liu, M., 2023. Spatial-temporal trajectory anomaly detection based on an improved spectral clustering algorithm. Intell. Data Anal. 27, 31–58.

Gupta, R., Tanwar, S., Tyagi, S., Kumar, N., 2020. Machine learning models for secure data analytics: a taxonomy and threat model. Comput. Commun. 153, 406–440.

Habeeb, R.A.A., Nasaruddin, F., Gani, A., Hashem, I.A.T., Ahmed, E., Imran, M., 2019. Real-time big data processing for anomaly detection: a survey. Int. J. Inf. Manag. 45, 289–307.

Han, X., Wang, Y., Zhang, X., Xu, N., 2023. Anomaly detection in time series satellite data using a deep learning method. In: 2023 CAA Symposium on Fault Detection, Supervision and Safety for Technical Processes (SAFEPROCESS). IEEE, pp. 1–6.

Harrison, T., Johnson, K., Roberts, T.G., 2019. Space Threat Assessment 2019. Center for Strategic & International Studies.

Hasan, R., Hasan, R., 2022. Towards a threat model and security analysis of spacecraft computing systems. In: 2022 IEEE International Conference on Wireless for Space and Extreme Environments (WiSEE). IEEE, pp. 87–92.

He, J., Cheng, Z., Guo, B., 2022a. Anomaly detection in satellite telemetry data using a sparse feature-based method. Sensors 22, 6358.

He, J., Cheng, Z., Xu, Z., Li, B., Liu, H., Guo, B., 2022b. Application of sparse representation method based on k-svd-admm in anomaly detection of satellite telemetry. In: 2022 Global Reliability and Prognostics and Health Management (PHM-Yantai). IEEE, pp. 1–7.

Hennecken, D.G., 2020. Beyza unal: cybersecurity of nato's space-based strategic assets. London: Chatham house, juli 2019. Sirius Z. Strateg. Anal. 4, 227–228.

Hills, G., Baldasare, J., Henry, W., Connell, W., 2022. A customized approach to cybersecurity education for space professionals. In: MILCOM 2022-2022 IEEE Military Communications Conference (MILCOM). IEEE, pp. 160–165.

Holmes, M., 2022a. Gauging the impact of satellite and space systems on critical infrastructure[CI]: risk management is neither an enigma nor a mystery for CI systems security. https://www.degruyter.com/document/doi/10.1515/jhsem-2022-0054/html?lang=en. (Accessed 20 June 2023) [Online].

Holmes, M., 2022b. The growing risk of a major satellite cyber attack. https://interactive.satellitetoday.com/the-growing-risk-of-a-major-satellite-cyber-attack/. (Accessed 20 June 2023) [Online].

Hou, Y., Li, H., Wang, Y., Wang, L., Xu, Z., 2023. Satellite anomaly detection based on improved transformer method. In: 2023 24th Asia-Pacific Network Operations and Management Symposium (APNOMS). IEEE, pp. 322–325.

Housen-Couriel, D., 2015. Cybersecurity and anti-satellite capabilities (asat) new threats and new legal responses. J. Law Cyber Warf. 4, 116–149.

Housen-Couriel, D., 2016. Cybersecurity threats to satellite communications: towards a typology of state actor responses. Acta Astronaut. 128, 409–415.

Housen-Couriel, D., 2023. Iac-21-e-9 (paper id: 67116) information sharing for the mitigation of outer space–related cybersecurity threats. Acta Astronaut. 203, 546–550.

Huang, Z., Wu, Y., 2022. A survey on explainable anomaly detection for industrial Internet of things. In: 2022 IEEE Conference on Dependable and Secure Computing (DSC). IEEE, pp. 1–9.
Hundman, K., Constantinou, V., Laporte, C., Colwell, I., Soderstrom, T., 2018. Detecting spacecraft anomalies using lstms and nonparametric dynamic thresholding. In: Proceedings of the 24th ACM SIGKDD International Conference on Knowledge Discovery & Data Mining, pp. 387–395.
Javaid, A.Y., Sun, W., Devabhaktuni, V.K., Alam, M., 2012. Cyber security threat analysis and modeling of an unmanned aerial vehicle system. In: 2012 IEEE Conference on Technologies for Homeland Security (hst). IEEE, pp. 585–590.
Jiang, H., Zhang, K., Wang, J., Wang, X., Huang, P., 2019. Anomaly detection and identification in satellite telemetry data based on pseudo-period. Appl. Sci. 10, 103.
Jin, W., Sun, B., Li, Z., Zhang, L., Zhang, S., 2021. Analytical investigation of anomaly detection methods based on time-domain features and autoencoders in satellite power subsystem. In: 2021 8th International Conference on Dependable Systems and Their Applications (DSA). IEEE, pp. 451–460.
Johnson, K., 2019. What is space security and why does it matter? Georget. J. Int. Aff. 20, 81.
Jones, H., 2018. The recent large reduction in space launch cost. In: International Conference.
Kaufman, M., Linzer, D., 2007. China criticized for anti-satellite missile test. Washington Post 19.
Kennewell, J.A., Vo, B.-N., 2013. An overview of space situational awareness. In: Proceedings of the 16th International Conference on Information Fusion. IEEE, pp. 1029–1036.
Khalil, S.M., Bahsi, H., Korõtko, T., 2023. Threat modeling of industrial control systems: a systematic literature review. Comput. Secur., 103543.
Kirshner, M., 2023. Model-based systems engineering cybersecurity for space systems. Aerospace 10, 116.
Knez, C., Llansó, T., Pearson, D., Schonfeld, T., Sotzen, K., 2016. Lessons learned from applying cyber risk management and survivability concepts to a space mission. In: 2016 IEEE Aerospace Conference. IEEE, pp. 1–8.
Kon, P.T.J., Barradas, D., Chen, A., 2022. Stargaze: a Leo constellation emulator for security experimentation. In: Proceedings of the 4th Workshop on CPS & IoT Security and Privacy, pp. 47–53.
Koroniotis, N., Moustafa, N., Slay, J., 2022. A new intelligent satellite deep learning network forensic framework for smart satellite networks. Comput. Electr. Eng. 99, 107745.
Korycki, L., Krawczyk, B., 2021. Class-incremental experience replay for continual learning under concept drift. In: Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition, pp. 3649–3658.
Korycki, Ł., Krawczyk, B., 2022. Adversarial concept drift detection under poisoning attacks for robust data stream mining. Mach. Learn., 1–36.
Kumar, M., Chand, S., 2020. A secure and efficient cloud-centric Internet-of-medical-things-enabled smart healthcare system with public verifiability. IEEE Int. Things J. 7, 10650–10659.
Kurakin, A., Goodfellow, I., Bengio, S., 2016. Adversarial machine learning at scale. ArXiv preprint. arXiv:1611.01236.
Kurt, M.N., Yılmaz, Y., Wang, X., 2020. Real-time nonparametric anomaly detection in high-dimensional settings. IEEE Trans. Pattern Anal. Mach. Intell. 43, 2463–2479.
Lang, K., Xu, B., Simon, M., Seibert, B., 2022. Automated satellite fault detection using machine learning. In: ASCEND 2022, p. 4297.
Langfu, C., Zhang, Q., Yan, S., Liman, Y., Yixuan, W., Junle, W., Chenggang, B., 2023. A method for satellite time series anomaly detection based on fast-dtw and improved-knn. Chin. J. Aeronaut. 36, 149–159.
Leao, B.P., Vempati, J., Muenz, U., Shekhar, S., Pandey, A., Hingos, D., Bhela, S., Wang, J., Bilby, C., 2022. Machine learning-based false data injection attack detection and localization in power grids. In: 2022 IEEE Conference on Communications and Network Security (CNS). IEEE, pp. 1–8.
Lee, M.-C., Nguyen, H.T., Berberidis, D., Tseng, V.S., Akoglu, L., 2021. Gawd: graph anomaly detection in weighted directed graph databases. In: Proceedings of the 2021 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining, pp. 143–150.
Lemos, R., 2001. Satellite control codes stolen by hackers.
Lewis, P. Livingstone, D., 2016. Space, the final frontier for cybersecurity. Recuperado el 24 2117492801–1495662736.
Leys, C., Klein, O., Dominicy, Y., Ley, C., 2018. Detecting multivariate outliers: use a robust variant of the Mahalanobis distance. J. Exp. Soc. Psychol. 74, 150–156.
Li, D., 2023. Cyber-attacks on space activities: revisiting the responsibility regime of article vi of the outer space treaty. Space Policy 63, 101522.
Li, H., He, J., Cheng, F., 2020. Research on Anomaly Detection Method for Satellite Power Supply Based on Bayesian Model. IOP Conference Series: Materials Science and Engineering, vol. 782. IOP Publishing, p. 032034.
Li, W., Mahadevan, V., Vasconcelos, N., 2013. Anomaly detection and localization in crowded scenes. IEEE Trans. Pattern Anal. Mach. Intell. 36, 18–32.
Li, Y., Lei, M., Liu, P., Wang, R., Xu, M., 2021a. A novel framework for anomaly detection for satellite momentum wheel based on optimized svm and huffman-multi-scale entropy. Entropy 23, 1062.
Li, Y., Wei, X., Li, Y., Dong, Z., Shahidehpour, M., 2022. Detection of false data injection attacks in smart grid: a secure federated deep learning approach. IEEE Trans. Smart Grid 13, 4862–4872.
Li, Z., Sun, B., Zhang, L., Jin, W., 2021b. Satellite on-2rbit anomaly detection and adaptive model updating method. In: 2021 8th International Conference on Dependable Systems and Their Applications (DSA). IEEE, pp. 647–655.
Liu, D., Pang, J., Song, G., Xie, W., Peng, Y., Peng, X., 2017. Fragment anomaly detection with prediction and statistical analysis for satellite telemetry. IEEE Access 5, 19269–19281.
Liu, L., Liu, H., Wang, E., Yu, T., Jia, S., Long, T., Sun, X., 2023a. Anomaly detection method of bds signal-in-space based on autoregressive distributed lag model. IEEE Access.
Liu, L., Tian, L., Kang, Z., Wan, T., 2023b. Spacecraft anomaly detection with attention temporal convolution network. arXiv:2303.06879.
Liu, M., Luo, T., Zhang, L., Cao, X., Duan, G., 2023c. An adjustable feature weighted bayesian model for hybrid satellite telemetry variables anomaly detection under multi-operating conditions. IEEE Trans. Instrum. Meas.
Liu, P., Zhang, H., Yuan, L., Zhang, B., Wang, C., 2022. Asynchronous autoregressive prediction for satellite anomaly detection. In: 2022 IEEE International Conference on Visual Communications and Image Processing (VCIP). IEEE, pp. 1–4.
Liu, P., Chen, L., Zhang, H., Zhang, Y., Liu, C., Li, C., Wang Pear, Z., 2023d. Positional-encoded asynchronous autoregression for satellite anomaly detection. Pattern Recognit. Lett.
Liu, Y., Pan, S., Wang, Y.G., Xiong, F., Wang, L., Chen, Q., Lee, V.C., 2021. Anomaly detection in dynamic graphs via transformer. IEEE Trans. Knowl. Data Eng.
Livingstone, D., Lewis, P., 2016. Space, the Final Frontier for Cybersecurity? Chatham House. The Royal Institute of International Affairs.
Llanso, T., Pearson, D., 2016. Achieving space mission resilience to cyber attack: architectural implications. In: AIAA SPACE 2016, p. 5604.
Luo, W., Liu, W., Gao, S., 2021a. Normal graph: spatial temporal graph convolutional networks based prediction network for skeleton based video anomaly detection. Neurocomputing 444, 332–337.
Luo, Y., Xiao, Y., Cheng, L., Peng, G., Yao, D., 2021b. Deep learning-based anomaly detection in cyber-physical systems: progress and opportunities. ACM Comput. Surv. (CSUR) 54, 1–36.
Ma, X., Wu, J., Xue, S., Yang, J., Zhou, C., Sheng, Q.Z., Xiong, H., Akoglu, L., 2021. A comprehensive survey on graph anomaly detection with deep learning. IEEE Trans. Knowl. Data Eng.
Malladi, C., 2017. Detection of objects in satellite images using supervised and unsupervised learning methods.
Manulis, M., Bridges, C.P., Harrison, R., Sekar, V., Davis, A., 2021. Cyber security in new space. Int. J. Inf. Secur. 20, 287–311.
Marsili, D., Boschetti, N., Gordon, N., Nikas, Y., Leger, W., Joyce, M., Falco, G., 2023. Slipping through attackers' fingers: fast neutron communications for space cybersecurity. In: 2023 IEEE Aerospace Conference. IEEE, pp. 1–12.
Martin, A.-S., 2023. Outer space, the final frontier of cyberspace: regulating cybersecurity issues in two interwoven domains. Astropolitics 21, 1–22.
Massimi, F., Ferrara, P., Benedetto, F., 2023. Deep learning methods for space situational awareness in mega-constellations satellite-based Internet of things networks. Sensors 23, 124.
Meraz, R., Vahala, L., 2020. Application of quantum cryptography to cybersecurity and critical infrastructures in space communications. OUR J.: ODU Undergrad. Res. J. 7, 5.
Mirchandani, S., Adhikari, S., 2020. Aerospace cybersecurity threat vector assessment. In: ASCEND 2020, p. 4116.
Mohamed, A.A., Chang, S.H., 2023. Sybil attack models of mm-wave communication for Leo satellite network in cybersecurity. In: 2023 International Conference on Consumer Electronics-Taiwan (ICCE-Taiwan). IEEE, pp. 281–282.
Mumcu, F., Doshi, K., Yilmaz, Y., 2022. Adversarial machine learning attacks against video anomaly detection systems. In: Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition, pp. 206–213.
Nalepa, J., Myller, M., Andrzejewski, J., Benecki, P., Piechaczek, S., Kostrzewa, D., 2022. Evaluating algorithms for anomaly detection in satellite telemetry data. Acta Astronaut. 198, 689–701.
Nassar, B., Hussein, W., Mokhtar, M., 2015. Space telemetry anomaly detection based on statistical pca algorithm. Int. J. Electron. Commun. Eng. 9, 637–645.
Nassif, A.B., Talib, M.A., Nasir, Q., Dakalbab, F.M., 2021. Machine learning for anomaly detection: a systematic review. IEEE Access 9, 78658–78700.
Niu, Z., Yu, K., Wu, X., 2020. Lstm-based vae-gan for time-series anomaly detection. Sensors 20, 3738.
Nizam, H., Zafar, S., Lv, Z., Wang, F., Hu, X., 2022. Real-time deep anomaly detection framework for multivariate time-series data in industrial iot. IEEE Sens. J. 22, 22836–22849.
Nussbaum, B., Berg, G., 2020. Cybersecurity implications of commercial off the shelf (cots) equipment in space infrastructure. In: Space Infrastructures: From Risk to Resilience Governance, pp. 91–99.
Oakley, J.G., 2020. Cybersecurity for Space: Protecting the Final Frontier. Apress.
Obied, M.A., Ghaleb, F.F., Hassanien, A.E., Abdelfattah, A.M., Zakaria, W., 2023. Deep clustering-based anomaly detection and health monitoring for satellite telemetry. Big Data Cogn. Comput. 7, 39.
Ogden, T., 2022. Satellite security in new space. https://airpower.airforce.gov.au/blog/BP27207741. (Accessed 20 June 2023) [Online].

Oh, M.-h., Iyengar, G., 2019. Sequential anomaly detection using inverse reinforcement learning. In: Proceedings of the 25th ACM SIGKDD International Conference on Knowledge Discovery & Data Mining, pp. 1480–1490.

OMeara, C., Schlag, L., Faltenbacher, L., Wickler, M., 2016. Athmos: automated telemetry health monitoring system at gsoc using outlier detection and supervised machine learning. In: 14th International Conference on Space Operations, p. 2347.

Pan, D., Song, Z., Nie, L., Wang, B., 2020. Satellite telemetry data anomaly detection using bi-lstm prediction based model. In: 2020 IEEE International Instrumentation and Measurement Technology Conference (I2MTC). IEEE, pp. 1–6.

Pavur, J., 2021. Securing new space: on satellite cyber-security. Ph.D. thesis. University of Oxford.

Pavur, J., Martinovic, I., 2019. The cyber-asat: on the impact of cyber weapons in outer space. In: 2019 11th International Conference on Cyber Conflict (CyCon), volume 900. IEEE, pp. 1–18.

Pavur, J., Martinovic, I., 2021. On detecting deception in space situational awareness. In: Proceedings of the 2021 ACM Asia Conference on Computer and Communications Security, pp. 280–291.

Pavur, J., Martinovic, I., 2022. Building a launchpad for satellite cyber-security research: lessons from 60 years of spaceflight. J. Cybersecurity 8, tyac008.

Pavur, J., Martinovic Sok, I., 2020. Building a launchpad for impactful satellite cyber-security research. ArXiv preprint. arXiv:2010.10872.

Pearson, J., 2022. Russia downed satellite Internet in Ukraine-western officials. Reuters 10.

Pedersen, J.K., Bøchman, M., Meng, W., 2022. Security analysis in satellite communication based on geostationary orbit. In: 2022 19th Annual International Conference on Privacy, Security & Trust (PST). IEEE, pp. 1–10.

Plotnek, J., Slay, J., 2022. New dawn for space security. In: International Conference on Cyber Warfare and Security, volume 17, pp. 253–261.

Poore, A.B., Aristoff, J.M., Horwood, J.T., Armellin, R., Cerven, W.T., Cheng, Y., Cox, C.M., Erwin, R.S., Frisbee, J.H., Hejduk, M.D., et al., 2016. Covariance and uncertainty realism in space surveillance and tracking. Technical Report. Numerica Corporation Fort Collins United States.

Popova, R., 2023. Space technology and cybersecurity: challenges and technical approaches for the regulation of large constellations. In: Space Law in a Networked World. Brill Nijhoff, pp. 102–128.

Presekal, A., Ştefanov, A., Rajkumar, V.S., Palensky, P., 2023. Attack graph model for cyber-physical power systems using hybrid deep learning. IEEE Trans. Smart Grid.

Ranshous, S., Shen, S., Koutra, D., Harenberg, S., Faloutsos, C., Samatova, N.F., 2015. Anomaly detection in dynamic networks: a survey. Wiley Interdiscip. Rev.: Comput. Stat. 7, 223–247.

Rendleman, J.D., Ryals, R., 2013. Cyber operations to defend space systems? In: AIAA SPACE 2013 Conference and Exposition, p. 5401.

Rettig, L., Khayati, M., Cudré-Mauroux, P., Piórkowski, M., 2019. Online anomaly detection over big data streams. In: Applied Data Science: Lessons Learned for the Data-Driven Business, pp. 289–312.

Robinson, J., 2016. Governance challenges at the intersection of space and cybersecurity. SECURING CYBERSPACE, p. 156.

Sabeti, E., Song, P.X., Hero, A.O., 2021. Data discovery using lossless compression-based sparse representation. In: ICASSP 2021-2021 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP). IEEE, pp. 5539–5543.

Sadr, M.A.M., Zhu, Y., Hu, P., 2023. Multivariate variance-based genetic ensemble learning for satellite anomaly detection. IEEE Trans. Veh. Technol.

Salkield, E., Szakály, M., Smailes, J., Köhler, S., Birnbach, S., Strohmeier, M., Martinovic, I., 2023. Satellite spoofing from a to z: on the requirements of satellite downlink overshadowing attacks. In: Proceedings of the 16th ACM Conference on Security and Privacy in Wireless and Mobile Networks, pp. 341–352.

Sanchez, S., Mazzolin, R., Kechaoglou, I., Wiemer, D., Mees, W., Muylaert, J., 2020. Cybersecurity space operation center: countering cyber threats in the space domain. In: Handbook Space Security. Springer, pp. 921–939.

Santangelo, A.D., 2021. The linkstar cybersecurity “sandbox”-a platform to test cubesat vulnerabilities within the small satellite community. In: ASCEND 2021, p. 4052.

Scholl, M., 2021. Introduction to cybersecurity for commercial satellite operations. Technical Report. National Institute of Standards and Technology.

Shen, M., Tang, X., Zhu, L., Du, X., Guizani, M., 2019. Privacy-preserving support vector machine training over blockchain-based encrypted iot data in smart cities. IEEE Int. Things J. 6, 7702–7712.

Shin, Y., Lee, S., Tariq, S., Lee, M.S., Jung, O., Chung, D., Woo, S.S., 2020. Itad: integrative tensor-based anomaly detection system for reducing false positives of satellite systems. In: Proceedings of the 29th ACM International Conference on Information & Knowledge Management, pp. 2733–2740.

Soize, C., 2017. Uncertainty Quantification. Springer.

Soligo, P., Merkel, G., Jorge, I., 2021. Ground segment anomaly detection using gaussian mixture model and rolling means in a power satellite subsystem. In: Argentine Congress of Computer Science. Springer, pp. 254–266.

Song, X., Aryal, S., Ting, K.M., Liu, Z., He, B., 2021. Spectral–spatial anomaly detection of hyperspectral data based on improved isolation forest. IEEE Trans. Geosci. Remote Sens. 60, 1–16.

Spanakis, E.G., Bonomi, S., Sfakianakis, S., Santucci, G., Lenti, S., Sorella, M., Tanasache, F.D., Palleschi, A., Ciccotelli, C., Sakkalis, V., et al., 2020. Cyber-attacks and threats for healthcare–a multi-layer thread analysis. In: 2020 42nd Annual International Conference of the IEEE Engineering in Medicine & Biology Society (EMBC). IEEE, pp. 5705–5708.

Studiawan, H., Payne, C., Sohel, F., 2017. Graph clustering and anomaly detection of access control log for forensic purposes. Digit. Investig. 21, 76–87.

Su, X., Xue, S., Liu, F., Wu, J., Yang, J., Zhou, C., Hu, W., Paris, C., Nepal, S., Jin, D., et al., 2022. A comprehensive survey on community detection with deep learning. IEEE Trans. Neural Netw. Learn. Syst.

Sun, H., He, F., Huang, J., Sun, Y., Li, Y., Wang, C., He, L., Sun, Z., Jia, X., 2020. Network embedding for community detection in attributed networks. ACM Trans. Knowl. Discov. Data 14, 1–25.

Tan, C., Sun, F., Kong, T., Zhang, W., Yang, C., Liu, C., 2018. A survey on deep transfer learning. In: Artificial Neural Networks and Machine Learning–ICANN 2018: 27th International Conference on Artificial Neural Networks, Rhodes, Greece, October 4-7, 2018, Proceedings, Part III 27. Springer, pp. 270–279.

Tanase, S., 2015. Satellite turla: Apt command and control in the sky. SecureList.

Tedeschi, P., Sciancalepore, S., Di Pietro, R., 2022. Satellite-based communications security: a survey of threats, solutions, and research challenges. Comput. Netw., 109246.

Thangavel, K., Plotnek, J.J., Gardi, A., Sabatini, R., 2022. Understanding and investigating adversary threats and countermeasures in the context of space cybersecurity. In: 2022 IEEE/AIAA 41st Digital Avionics Systems Conference (DASC). IEEE, pp. 1–10.

Triscari, C., 2022. Space technology in Australia. https://apo.org.au/node/319476.

Tritscher, J., Krause, A., Hotho, A., 2023. Feature relevance xai in anomaly detection: reviewing approaches and challenges. Front. Artif. Intell. 6, 7.

Truong, H.T., Ta, B.P., Le, Q.A., Nguyen, D.M., Le, C.T., Nguyen, H.X., Do, H.T., Nguyen, H.T., Tran, K.P., 2022. Light-weight federated learning-based anomaly detection for time-series data in industrial control systems. Comput. Ind. 140, 103692.

Tsai, C.-C., Sun, C.-Y., Yang, S.-H., 2023. Note on “raks: robust authentication and key agreement scheme for satellite infrastructure”. In: 2023 International Conference on Consumer Electronics-Taiwan (ICCE-Taiwan). IEEE, pp. 291–292.

Tsamis, N., Bailey, B., Falco, G., 2021. Translating space cybersecurity policy into actionable guidance for space vehicles. In: ASCEND 2021, p. 4051.

Unal, B., 2019. Cybersecurity of NATO’s Space-Based Strategic Assets, Chatham House. The Royal Institute of International Affairs.

Vanini, P., Rossi, S., Zvizdic, E., Domenig, T., 2023. Online payment fraud: from anomaly detection to risk management. Financ. Innov. 9, 1–25.

Varadharajan, V., 2022a. Security challenges when space merges with cyberspace. https://www.newcastle.edu.au/_data/assets/pdf_file/0003/818211/Security-Challenges-when-Space-Merges-with-Cyberspace.pdf. (Accessed 20 June 2023) [Online].

Varadharajan, V., 2022b. Security challenges when space merges with cyberspace. https://arxiv.org/ftp/arxiv/papers/2207/2207.10798.pdf. (Accessed 20 June 2023) [Online].

Velasco-Gallego, C., Lazakis, I., 2022. Radis: a real-time anomaly detection intelligent system for fault diagnosis of marine machinery. Expert Syst. Appl. 204, 117634.

Vessels, L., Heffner, K., Johnson, D., 2019. Cybersecurity risk assessment for space systems. In: 2019 IEEE Space Computing Conference (SCC). IEEE, pp. 11–19.

Viswanathan, A., Pecharich, J., 2016. The new space race: cyber security for space missions. NASA.

Vivero, J., 2013. Space missions cybersecurity modelling. In: 31st AIAA International Communications Satellite Systems Conference, p. 5634.

Wang, J., Jia, Y., Wang, D., Xiao, W., Wang, Z., 2022a. Weighted iforest and Siamese gru on small sample anomaly detection in healthcare. Comput. Methods Programs Biomed. 218, 106706.

Wang, J., Li, H., Wang, L., Xu, Z., 2023. Satellite telemetry data anomaly detection using multiple factors and co-attention based lstm. In: 2023 IEEE Wireless Communications and Networking Conference (WCNC). IEEE, pp. 1–6.

Wang, Y., Wu, Y., Yang, Q., Zhang, J., 2021. Anomaly detection of spacecraft telemetry data using temporal convolution network. In: 2021 IEEE International Instrumentation and Measurement Technology Conference (I2MTC). IEEE, pp. 1–5.

Wang, Y., Gong, J., Zhang, J., Han, X., 2022b. A deep learning anomaly detection framework for satellite telemetry with fake anomalies. Int. J. Aerosp. Eng. 2022, 1–9.

Wazid, M., Das, A.K., Shetty, S., Rodrigues, J.J., Guizani, M., 2022. Aiscm-fh: Ai-enabled secure communication mechanism in fog computing-based healthcare. IEEE Trans. Inf. Forensics Secur. 18, 319–334.

Widhalm, D., Goeschka, K.M., Kastner Sok, W., 2020. A taxonomy for anomaly detection in wireless sensor networks focused on node-level techniques. In: Proceedings of the 15th International Conference on Availability, Reliability and Security, pp. 1–10.

Wright, D., Grego, L., Gronlund, L., 2005. The physics of space security. In: A Reference Manual. Cambridge.

Wu, J., Yao, L., Liu, B., Ding, Z., Zhang, L., 2020. Combining oc-svms with lstm for detecting anomalies in telemetry data with irregular intervals. IEEE Access 8, 106648–106659.

Xie, L., Pi, D., Zhang, X., Chen, J., Luo, Y., Yu, W., 2021. Graph neural network approach for anomaly detection. Measurement 180, 109546.

Xu, Z., Cheng, Z., Guo, B., 2022. An lstm autoencoder-based framework for satellite telemetry anomaly detection. In: 2022 4th International Conference on System Reliability and Safety Engineering (SRSE). IEEE, pp. 231–234.

Yang, G., Ye, Q., Xia, J., 2022. Unbox the black-box for the medical explainable ai via multi-modal and multi-centre data fusion: a mini-review, two showcases and beyond. Inf. Fusion 77, 29–52.
Yoo, Y., Lee, C.-Y., Zhang, B.-T., 2021. Multimodal anomaly detection based on deep auto-encoder for object slip perception of mobile manipulation robots. In: 2021 IEEE International Conference on Robotics and Automation (ICRA), pp. 11443–11449.
Yu, B., Zhang, Y., Xie, W., Zuo, W., Zhao, Y., Wei, Y., 2023. A network traffic anomaly detection method based on Gaussian mixture model. Electronics 12, 1397.
Yu, W., Cheng, W., Aggarwal, C.C., Zhang, K., Chen, H., Wang, W., 2018. Netwalk: a flexible deep embedding approach for anomaly detection in dynamic networks. In: Proceedings of the 24th ACM SIGKDD International Conference on Knowledge Discovery & Data Mining, pp. 2672–2681.
Yue, P., An, J., Zhang, J., Pan, G., Wang, S., Xiao, P., Hanzo, L., 2022. On the security of Leo satellite communication systems: vulnerabilities, countermeasures, and future trends. ArXiv preprint. arXiv:2201.03063.
Yuqing, L., Tianshe, Y., Xueliang, C., Rixin, W., Minqiang, X., 2016. An anomaly detection algorithm of satellite power system based on cusum control chart. In: 2016 3rd International Conference on Information Science and Control Engineering (ICISCE). IEEE, pp. 829–833.
Zardi, H., Karamti, H., Karamti, W., Alghamdi, N.S., 2022. Detecting anomalies in network communities based on structural and attribute deviation. Appl. Sci. 12, 11791.
Zatti, S., 2017. The protection of space missions: threats and cyber threats. In: Information Systems Security: 13th International Conference, ICISS 2017, Mumbai, India, December 16-20, 2017, Proceedings 13. Springer, pp. 3–8.
Zeng, Z., Jin, G., Xu, C., Chen, S., Zeng, Z., Zhang, L., 2022. Satellite telemetry data anomaly detection using causal network and feature-attention-based lstm. IEEE Trans. Instrum. Meas. 71, 1–21.
Zhao, H., Wang, Y., Duan, J., Huang, C., Cao, D., Tong, Y., Xu, B., Bai, J., Tong, J., Zhang, Q., 2020. Multivariate time-series anomaly detection via graph attention network. In: 2020 IEEE International Conference on Data Mining (ICDM). IEEE, pp. 841–850.
Zhao, H., Liu, M., Qiu, S., Cao, X., 2023. Satellite unsupervised anomaly detection based on deconvolution-reconstructed temporal convolutional autoencoder. IEEE Trans. Consum. Electron.
Zheng, L., Li, Z., Li, J., Li, Z., Gao, J., 2019. Addgraph: anomaly detection in dynamic graph using attention-based temporal gcn. In: IJCAI, volume 3, p. 7.
Zhou, L., Zeng, Q., Li, B., 2022. Hybrid anomaly detection via multihead dynamic graph attention networks for multivariate time series. IEEE Access 10, 40967–40978.
Zhou, Z.-G., Tang, P., 2016. Continuous anomaly detection in satellite image time series based on z-scores of season-trend model residuals. In: 2016 IEEE International Geoscience and Remote Sensing Symposium (IGARSS). IEEE, pp. 3410–3413.
Zhu, D., Ma, Y., Liu, Y., 2020. A flexible attentive temporal graph networks for anomaly detection in dynamic networks. In: 2020 IEEE 19th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom). IEEE, pp. 870–875.
Zhuo, M., Liu, L., Zhou, S., Tian, Z., 2021. Survey on security issues of routing and anomaly detection for space information networks. Sci. Rep. 11, 1–18.
Žunić, E., Tucaković, Z., Hodžič, K., Delalić, S., 2019. Multi-level generalized clustering approach and algorithm for anomaly detection in internal banking payment systems. In: IEEE EUROCON 2019-18th International Conference on Smart Technologies. IEEE, pp. 1–6.

Dr **Abebe Diro** is a lecturer at RMIT University's School of Accounting, Information Systems and Supply Chain. He is a cyber security scientist with interests in machine learning-based cyber security, and cryptography. He has made outstanding contributions to these fields with publications in high-quality journals. The research outputs include pioneering work on distributed machine learning for intrusion detection in the Internet of Things. Further, Dr Diro has proven his ability to establish relevant research collaborations with industry through various projects, which is supported by RMIT University's emphasis on aligning research with areas of national interest. He has also established collaborations with academics in Europe, Australia, South Korea, Indonesia, and Turkey, where he has co-published journal articles with researchers. His high-quality research in cyber security and his extensive research networks in cyber security and cryptography mark him as a leading researcher at RMIT.

Dr **Shahriar Kaisar** is a lecturer in the Department of Information Systems and Business Analytics at RMIT University. He obtained his Ph.D. from Monash University's faculty of information technology and his master's degree from the University of Saskatchewan in Canada. Dr. Kaisar's research focuses on business analytics, emerging technologies, cybersecurity, and health informatics. He is actively engaged in exploring the intersection of these fields and their implications for organizations and society.

Prof **Athanasios V. Vasilakos** is with the Center for AI Research (CAIR), University of Agder (UiA), Grimstad, Norway. He served or is serving as an Editor for many technical journals, such as the IEEE Transactions on AI, IEEE Transactions on Network and Service Management; IEEE Transactions on Cloud Computing, IEEE Transactions on Information Forensics and Security, IEEE Transactions on Cybernetics; IEEE Transactions on Nanobioscience; IEEE Transactions on Information Technology in Biomedicine; ACM Transactions on Autonomous and Adaptive Systems; IEEE Journal on Selected Areas in Communications. He is a WoS highly cited researcher (HC).

Dr **Adnan Anwar** is a Cyber Security academic at Deakin University and a member of the Centre for Cyber Security Research and Innovation (CSRI). With over 10 years of experience in industrial, research, and teaching positions at universities and research labs such as NICTA (now Data61 of CSIRO), UNSW, La Trobe University, and Deakin University, he has a wealth of knowledge in the field. He received his PhD and Master by Research from UNSW at the Australian Defence Force Academy (ADFA). With an H-index of 24, he has published over 100 articles in prestigious journals, conference articles, and book chapters. He has secured funding for his research from government, defense, and industries and has received several awards for excellence in research and teaching at Deakin. Dr. Anwar's research has greatly advanced the field of artificial intelligence and data-driven cybersecurity for critical infrastructure in Australia, while his teaching has helped produce the next generation of Australian data analytics experts in security and privacy.

Dr **Araz Nasirian** is a Lecturer in the Department of Information Systems and Business Analytics at RMIT University. He holds a Ph.D. in data science and business analytics, achieved in 2020, and a Master's degree in project management earned in 2015. His research interests lie in optimization and artificial neural networks, with his work published in A* journals. Dr. Nasirian's industry experience includes serving as an analytics advisor in a business intelligence company. He specializes in developing user-friendly applications for data analysis and received the RMIT University Vice Chancellor Award for Excellence in 2022. He has developed numerous courses on data science and business analytics for students and industry practitioners.

Dr. **Gaddisa Olani** is a highly accomplished researcher and academic in the field of computer science. He is an active member of the Institute of Electrical and Electronics Engineers (IEEE). Dr. Olani completed his bachelor's degree in computer science and IT at Wollega University, Ethiopia, in 2010,followed by a master's degree in computer science from Addis Ababa University in 2013. In 2020, he earned his Ph.D. from the Social Network Analysis and Human-Centered Computing Department at National Tsing Hua University and Academia Sinica, Taiwan. From September 2010 to July 2017, Dr. Olani served as a Lecturer in the Department of Computer Science at Dire Dawa University in Ethiopia. Currently, he holds the position of Assistant Professor of computer science at the School of Computing, Department of Computer Science, Dire Dawa University. Dr. Olani was awarded a prestigious scholarship by the Taiwan International Graduate Program (TIGP) to pursue his Ph.D. studies at NTHU. His research interests encompass various areas, including big data analysis, cybersecurity, AI-based intrusion detection systems, natural language processing, and user behavior modelling for cyber deceptions.