Space Spider: A Hyper Large Scientific Infrastructure Based On Digital Twin For The Space Internet

Jiaqi Li
Institute of Information Engineering, Chinese Academy of Sciences
Haidian Qu, Beijing Shi, China
lijiaqi@iie.ac.cn

Lvyang Zhang
Institute of Information Engineering, Chinese Academy of Sciences
Haidian Qu, Beijing Shi, China
zhanglvyang@iie.ac.cn

Quan Hong
Institute of Information Engineering, Chinese Academy of Sciences
Haidian Qu, Beijing Shi, China
hongquan@iie.ac.cn

Yang Yu
Tencent Security Xuanwu Lab
Haidian Qu, Beijing Shi, China
tkyu@Tencent.com

Lidong Zhai
Institute of Information Engineering, Chinese Academy of Sciences
Haidian Qu, Beijing Shi, China
zhailidong@iie.ac.cn

ABSTRACT

With its advantages of low latency and global coverage, the Low Earth Orbit (LEO) satellite constellations can form an effective complement to the terrestrial 5G/6G mobile communication system and provide infrastructure support for broadband access and various services of the Internet. However, due to the spatial particularity of this network across land, sea, air, and other levels, it faces the dilemma of being "easy to attack" and "difficult to defend". At the same time, with the acceleration of the wave of digital transformation, the space Internet is increasingly facing software supply chain security risks. Currently, there is no security simulation and verification platform for the whole life cycle of the space Internet. Therefore, in the present study, we design a digital twin-based hyper large scientific infrastructure for the space Internet named Space Spider to realize the ground simulation of all elements of the space Internet and establish an attack and defense environment for the space Internet to support core technology verification. In addition, we also proposed Spiderland, an open experimental platform for space Internet applications and security researchers, to conduct simulation and attack-defense experiments.

CCS CONCEPTS

• **Security and privacy** → **Network security**; **Mobile and wireless security**; • **General and reference** → **Design**; **Experimentation**.

KEYWORDS

hyper large scientific infrastructure, digital twin, space internet, space range

ACM Reference Format:
Jiaqi Li, Lvyang Zhang, Quan Hong, Yang Yu, and Lidong Zhai. 2022. Space Spider: A Hyper Large Scientific Infrastructure Based On Digital Twin For The Space Internet. In *1st Workshop on Digital Twin & Edge AI for IIoT (Digital Twin & Edge AI for Industrial IoT '22), October 17, 2022, Sydney, NSW, Australia.* ACM, New York, NY, USA, 6 pages. https://doi.org/10.1145/3566099.3569007

Digital Twin & Edge AI for Industrial IoT '22, October 17, 2022, Sydney, NSW, Australia

ACM ISBN 978-1-4503-9784-1/22/10.
https://doi.org/10.1145/3566099.3569007

1 INTRODUCTION

Companies like SpaceX Starlink, Amazon Kuiper, and others are deploying hundreds or thousands of satellites. Space Internet is an excellent supplement to optical fiber and mobile Internet as an emerging network mode. The Low Earth Orbit (LEO) constellation not only bridges the digital divide by providing services to remote areas but also offers lower latency than terrestrial fiber for long-distance transmission. The core application scenarios of the space Internet are extensive, which can realize the early warning of extreme weather disasters such as river water level flow, agricultural pests, diseases, earthquakes, forest fires, etc., and discover the real-time distribution and control of power facilities and lines in remote areas. The research and development of LEO are increasingly valued by academia and industry, motivated by this great potential.

However, the development of the space Internet is also facing a severe risk , not only "easy to attack" but also "difficult to defend". Large-scale small satellites in the space Internet, especially the tiny CubeSat satellites, use industrial assembly line technology to reduce costs, which means that hackers may implant backdoors and other vulnerabilities into satellite software, which poses a substantial technical security risk. In 2021, Giacomo Giuliari et al. successfully attacked low-Earth orbit satellite networks by analyzing the vulnerability of satellite networks to DOSS attacks and proposing an attack model called ICARUS. In 2022, hackers disabled modems for the Ka-SAT satellite of the US telecommunications company Viasat, causing the destruction of broadband space Internet access in Ukraine and the disconnection of tens of thousands of European Internet users.

In addition, it is also facing the dilemma of being "difficult to defend". The distance of satellite transmission is very long, and it is affected by the speed of the light delay effect, frame loss, and packet loss. The computing and storage functions are also limited, making it difficult for the current satellite communication transmission to apply high reliability and high-strength encryption transmission methods like terrestrial communication. Satellite network nodes in the continuous high-speed movement lead to frequent switching of

links, resulting in frequent changes in topology, which also leads to the existing ground network defense methods are not fully applicable to the defense of satellite networks. Once the satellite network is breached, it will cause severe consequences to the country and society.

Except for the security risks brought by the nature of the space Internet, software supply chain security risks will be a crucial issue in the future, with the acceleration of the wave of digital transformation. The Apache Log4j vulnerability is one of the most egregious vulnerabilities in the history of the Internet, and, inevitably, the current large-scale use of space Internet scientific research software, business software, and application software may face similar risks. However, this trend is not highly regarded by non-cybersecurity practitioners.

Faced with the security risks in the space Internet, we have proposed a new technical route, promoted "security first", established experimental beds on the ground in advance, and designed the overall solution of space Internet from the perspective of safety. Given the problems of high construction cost and the long cycle of the test environment of the space Internet, a large-scale simulation and verification platform named Space Spider based on digital twin is established on the ground side, including the simulation of large-scale satellite constellation operation, networking, multi-form communication, and typical space Internet business scenarios, to realize the ground reproduction of all elements of the space Internet. On top of it, the principle and effect verification of new technologies related to the space Internet is carried out.

Using the physical thought from the particular to the general, we believe that this space Internet simulation and verification platform should be defined as a hyper large scientific infrastructure [11]. Through scientific research and analysis of traditional large scientific infrastructures, we extracted the ten core characteristics of the attribution of large scientific infrastructures. Further, the space Internet attack-defense simulation and verification platform should be a hyper large scientific infrastructure based on traditional large scientific infrastructures. This transcendence is not limited to the expansion of scale (super), nor yet the speculation of its essence (meta) in metaphysics without empirical evidence, but belongs to the spiral of evolution (hyper) in the field of natural sciences.

In conclusion, this paper makes the following contributions:

1. The characteristics of traditional large scientific infrastructures are systematically sorted out, and the hyper large scientific infrastructures and evaluation indicators are creatively defined.

2. Given the security risks faced by the space Internet, the construction of Space Spider, it is proposed to build a hyper large scientific infrastructure for the space Internet, conduct a homologous simulation of the whole life cycle elements of the space Internet, and construct simulation objects for experimental verification, to build a space Internet attack and defense capability system.

3. Spiderland, an open experimental platform for the space Internet, is developed to provide an experimental platform for practitioners and researchers of the space Internet application and security and interested people to research the space Internet application and deposit.

The rest of the paper is structured as follows. In Section II, we briefly reviewed the space Internet security-related work. In Section III, we define a hyper large scientific infrastructure. In Section IV, we introduce Space Spider, a hyper large scientific infrastructure for the space Internet. Section V presents Spiderland, an open platform for the space Internet. In Section VI, we summarize this paper.

2 RELATED WORK

In this section, we sort out and summarize the related work in the field of space Internet, including space Internet security and space Internet simulation platform.

2.1 Space Internet Security

The space Internet has the characteristics of numerous network nodes, open channel links, and complex topological structures. The previous encryption methods of satellite communication are not appropriate for the satellite network with authoritarian and available satellite node structures. Therefore, it is urgent to have a unique security network architecture for the space Internet.

In order to respond to the threat of passive and active attack, Yan et al. [16] analyzed for aspects of the current satellite security technology, according to the functional characteristics satellite network. Cao et al. [1] summarizes 13 safety problems by the satellite network security risk analyzed from the perspective of national security, network security and equipment security to provide reference for the healthy development of the space Internet industry. Zhu et al. [18] proposed intersatellite networking scheme applicable to the two-layer satellite network. This schemes make use of the characteristics of high unity of satellite clock and predictability of running trajectory, to ensure secure communication between orbits and satellites, under the case of no third reliable party involved. Li et al. [7] put forward a SAGIN security guarantee architecture which combined security layer, security support layer, network security layer, security service layer, security situation warning, and unified security management, etc. Zhang et al. [17] proposed a dynamic enabling architecture of space-air-ground integrated information network security, which mixed security service capability arrangement, security situation analysis, and security threat disposal command, etc.

The space Internet has the dual attributes of the Internet and mobile communication, which is essential to realizing the vision of "connecting everything". Furthermore, the development of the space Internet requires the coordinated promotion of multiple industries and fields, including satellite design and manufacturing, satellite launch, satellite communication, and network security. However, it faces several fundamental problems, such as regulatory difficulties, security enhancement, satellite collision avoidance, communication interference control, constellation unity and coordination, satellite confrontation, etc., and urgently needs to make technological breakthroughs.

2.2 Space Internet Simulation Platform

The space Internet includes three network segments: satellite system, air network and ground communication [9]. So far, most of the existing research work has focused on analog space, air or a single ground network segment. Tapsawat et al.[14] developed a low-cost hardware-in-the-loop (HIL) simulator for testing ADCS of CubeSat satellites. Ma et al.[12] proposed a reinforcement learning method to re-stabilize the satellite's attitude in this situation. The

proposed control scheme is applied to the damping mode of the satellite and the simulation results are compared with the gyroscope measurement data. Li et al.[8] and Du et al.[3] put forward a space surveillance satellite with a mission to detect, catalog and maintain space debris as small as 10 centimeters in the geosynchronous Earth orbit (GEO) region. In view of the actual needs of the current satellite communication system application, Mao et al.[13] advanced a HLA-based satellite communication application multi-dimensional interactive simulation system (MDIS) scheme and simulation method. Liu et al.[10] imported a lightweight, all-in-one simulation platform for large and small satellite networks. Tian et al.[15] built a simulation model of ground target positioning based on the determination of the on-board direction. Based on public details in the FCC filing, Handley et al.[5] built a simulator using unity3D to evaluate how to use laser links to provide a network and to study routing problems on the network. Giuliari et al.[4] designed a custom simulator to simulate the number of ground station deployments and the connectivity and latency caused by the space Internet in rainy conditions. Cheng et al.[2] introduced the developed SAGIN simulation platform that supports various movement trajectories and protocols for space, air and terrestrial networks.

The space Internet is different from terrestrial networks. There are two main differences: one is point-to-point long-distance wireless communication; the other is the regular movement of nodes. Both are unavailable in terrestrial wireless networks (e.g., Ad-hoc, LTE, etc.). However, there is currently no mature satellite network simulation platform. Before conducting relevant research, we cannot wait until the low-orbit space Internet is finished. To this end, it is high time that we established a unique simulation and verification platform for the space Internet to realize ground simulation, technical verification, attack and defense exercises, service access, and standards development for all elements of the space Internet.

3 HYPER LARGE SCIENTIFIC INFRASTRUCTURE

We believe that this attack and defense simulation and verification platform for the space Internet should be designed as a hyper large scientific infrastructure. In June 1962, the American scientist Price gave a lecture entitled "Small Science, Big Science", which mentioned that the world had entered the era of "big science" since the Second World War. However, there is no single definition of a big Science installation. For example, the US Department of Energy defines it as LargeScale Scientific Instrumentation. The German Research Centre for Electron Synchrotron (DESY) defines it as a Large-scale facility for science. The construction process of a large scientific device is a process of infinite convergence. In the process, problems are constantly solved, and the uncertainty is finally changed into certainty. Its core connotation lies in the complexity of the device, the foundation of multidisciplinary application support, and the specificity. Large scientific devices should be compatible, timely, and systematic in the long run. Through the unified scientific research and analysis of typical large scientific devices, we extract four essential attributes and ten core features of the attribution of large scientific instruments, described in the following.

The four essential attributes of an extensive scientific infrastructure is summarized as SCDE, which are ordered in order of consideration of construction principles, namely S (Scientification), C (Connotation), D (Designing), and E (Evaluative).

S: Scientificity, Determinism;
C: Complexity, Proprietary, Fundamental;
D: Systematicity, Compatibility, Timeliness;
E: Leadership, Economy.

From the above characteristic paradigms, the more complete the coverage degree, the stronger the coverage capability, and the higher the maturity of large scientific infrastructure. The space Internet attack and defense simulation and verification platform should be a hyper large scientific infrastructure based on the traditional large scientific infrastructure. In addition to the above ten core characteristics, it also has two subjective characteristics of Spatio-temporal transcendence and continuous evolution.

Spatio-temporal transcendence: Spatio-temporal transcendence should be comprehended in two dimensions: time and space. Time is retrospective, and space is connected, collectively called Spatio-temporal transcendence. It can be upward compatible with the Metaverse, downward compatible with 4G, aerospace, safety range, parallel compatible nuclear power plants, and other industries.

Continuous evolution: Continuous evolution refers to an advanced system that consistently maintains vitality and keeps pace with the times, which can achieve self-improvement of methodologies, strategy sets, and even its supporting theory according to the evolution of cutting-edge technologies.

The hyper large scientific infrastructures can evolve upwards, and their application scenarios can be extended to a larger space, namely the Metaverse. The spacetime view of traditional large scientific infrastructures is based on an actual carrier. While the space-time view of hyper large scientific installations has been upgraded, and its digital twin in the meta-universe and even the mapping of other parallel universes are enough to carry the possibility of its multi-channel, multi-directional, and multi-space radiation, which is the essential innovation of the upward evolution of the space-time view.

The hyper large scientific infrastructures can be backward compatible, and they can be consistent with 4G communication. New features beyond large scientific infrastructure: Spatio-temporal transcendence aerospace, safety shooting range, and parallel compatibility with various industries such as nuclear power plants. With the development of the economy, the hyper large scientific infrastructures have the natural attributes and ability to track the direction of the digital economy accurately, represent the progress direction of human social civilization, and follow the path of economic development with real-time feedback adjustment and self-calibration.

The hyper large scientific infrastructures can also realize parallel mapping. With the explosive development of the infrastructure construction of the Metaverse, human communities similar to the earth will be formed naturally or artificially in parallel universes. Human social and economic development activities in such communities. It is an excellent practice of the concept of a parallel universe. The hyper large scientific infrastructure can radiate to other planets and their affiliated parallel universes and then incorporate these parallel universes into the system ecology of the hyper large scientific

infrastructure, taking space as a whole and synergizing to drive the social and economic development of the "humanoid" community.

4 SPACE SPIDER

4.1 Overview

Currently, there is no new technology for the space Internet for the whole life cycle verification environment. To reduce the network security risks of the space Internet, based on ensuring the regular and effective operation of the existing network security protection system, from the overall perspective, we propose a simulation and verification hyper large scientific infrastructure architecture specially oriented to the space Internet, and named it "Space Spider" to realize ground simulation, technical verification, and attack-defense exercises of all elements of the space Internet.

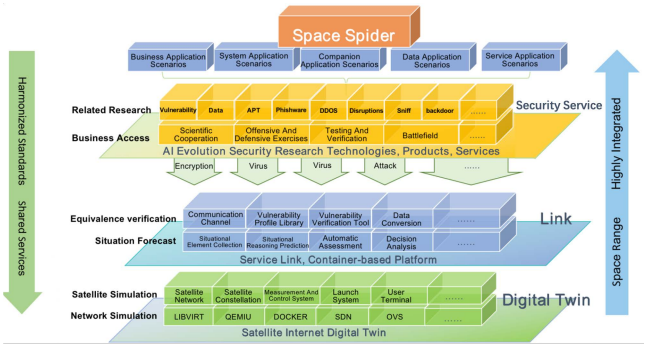

Figure 1: Technical Architecture of the Space Spider

4.2 Technical Architecture

4.2.1 Digital twin layer. The digital twin layer provides infrastructure support for the security guarantee service of the hyper large scientific infrastructure for space Internet, including the digital twin of space, the digital twin of network, and network defense architecture.

The digital twin of space refers to the virtual construction of the whole life cycle of satellites in the time dimension based on the physical world, the digital world, and the human world, taking time and space as the baseline, including overall satellite design, satellite detail design, satellite manufacturing, a satellite launch, satellite in-orbit operation, satellite management, etc. In the space dimension, taking space as the scene, the environment such as satellites, rockets, radars, aircraft, ground stations, and launch sites, as well as activity information such as measurement and operation control, remote sensing, communication, navigation, and early warning, is expressed in a digital way to build a digital space that meets general or specific needs.

The digital twin of network aims to unify the dispatch of available resources in different network nodes. According to additional network requirements, the available resources of all nodes in the space Internet are reorganized and allocated, thus breaking through the physical constraints of non-interoperability between satellite nodes in different satellite constellations or constellations and reducing the overhead of satellite network deployment and management. Meanwhile, service slice samples composed of other virtualized network functions in the resource pool are orchestrated to meet users' requirements for different service quality.

The network defense adopts the active defense architecture based on Shock Trap [6]. It belongs to the application of the guard mode in operational defense. The technical idea is to deploy a trap protection layer at the outer layer of the program to protect the security of the system. In addition, Shock Trap is different from other defense technologies. Instead of fixing vulnerabilities, its focus is on deploying traps in systems to trick, track, and deter attackers. The defense process is shown in Figure 2. We combined Shock Trap with hyper large scientific infrastructure because this trap-based protection mode is passively triggered and has low occupancy. It can guarantee the system security of the hyper large scientific infrastructures without affecting regular operation.

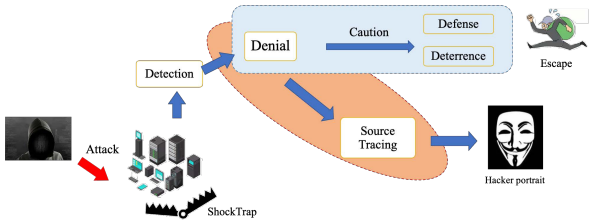

Figure 2: The Active Defense Mechanism of ShockTrap

4.2.2 Link layer. The link layer is the connection between the security services of Space Spider and the overall infrastructure of the space Internet, including security situational awareness and equivalence verification. Security situational awareness refers to understanding environmental factors in a specific time and space and predicting future trends. Equivalence verification refers to the analogous adaptation of known terrestrial security risks to space Internet security.

Security situational awareness includes three components: data import, data processing and analysis, and security situational presentation. The data ingress layer collects data through built-in devices such as threat-driven traffic data (mainly recording packet time, IP address, port, protocol information, etc.), log collector (specifically collects policy logs, alarm logs, operation logs, status information, etc.), and asset detectors (mainly contains asset types, IP addresses, operating systems, software versions, protocols, services, open ports, and other information). The data information is aggregated to the safety data bus via API calls. Data processing and analysis is responsible for managing data resources, association relationships, and other information and first normalizing the data. Then, use the existing knowledge of models and strategies to complete the construction of the database, generate data correlation information, realize data fusion, and enhance data value. Finally, combined with the existing knowledge base information, the analysis model is constructed through analysis and mining to complete the update and accumulation of the knowledge base and provide intelligent support for data processing and services. Security posture presentation refers to the data results collected, processed, analyzed, and transformed into clear curve charts with

the help of situational awareness system software and visualization technology to visualize security events, attack paths, and regions and reduce the difficulty of operation and maintenance.

In equivalence verification, "equivalence" refers to a system in an approximate environment under actual or near-real-world application conditions. According to the user's requirements, a comprehensive technical specifications check is carried out in an actual or near-real-world application environment to verify whether the technical specifications meet the expected requirements. The critical issue to consider in "Validation" is to check that the specifications meet the requirements. The development of the global space Internet industry is gradually entering the fast lane, and countries are also entering a period of intensive deployment. However, the network has not yet been completed. The integrated planning and construction steps have yet to be studied in depth. The follow-up construction process will face many difficulties, such as communication standards, information security, and industrial applications. Therefore, for a long time to come, the space Internet will still be in the construction stage. Is the space Internet a "paper tiger" or a "new version" of the traditional internet? Therefore, we must verify whether the space Internet is equivalent to the established terrestrial Internet. The main areas of verification are as follows.

(1) Whether the communication protocols, standards, and topologies of the traditional Internet apply to the space Internet.

(2) Whether the traditional Internet's attack methods and means apply to the space Internet?

(3) Whether the security protection measures of the traditional Internet apply to the space Internet.

4.2.3 Security service layer. The security service layer is suitable for scientific research, real-world confrontation, and emergency exercise.

Scientific research mainly carries out vulnerability mining and risk verification. Based on the automatic business scenario construction capability, physical simulation capability, and virtual-real combination capability of Space Spider, a vulnerability mining business system for software and hardware is built, and satellite devices such as satellite terminals and satellite measurement, operation, and control equipment are realized. Vulnerability mining of IT equipment such as switches and servers, or professional software and hardware equipment such as programmable logic controllers (PLCs) and distributed control systems (DCS). Risk verification uses the vulnerability and risk resource library as the technical support to test and diagnose the target system/device, identify system device information, test the system's vulnerability, analyze known vulnerabilities, mine unknown vulnerabilities, and generate alarms and system analysis reports.

The competition provides pre-set ultra-realistic network security scenarios, each pre-injected with vulnerabilities and fragility so that users can use the scenarios for attack-defense confrontation exercises and trials. At the same time, advanced technologies and concepts such as big data and artificial intelligence are introduced to enhance the competition evaluation and strengthen the training effect of the teaching range.

The real-world confrontation can support a variety of real-world exercise modes. The intrusion exercise supports simulated attacks on specific scenarios and executes attacks from various entry points within a limited time frame. Defense exercises are responsible for defending the network and its critical assets and focus on training defenders, identifying and countering attack scenarios, and developing real-world experience. The confrontation exercise adopts the actual combat training mode. A team of attackers and defenders is assigned to a highly simulated exercise scenario in which both sides perform attack and defense confrontation-type operations according to their respective tasks.

The emergency exercise is a training platform for training the capabilities of emergency personnel. It is built around the core functions of deduction control, deduction evaluation, and multi-role collaborative deduction, and an online practical exercise environment is established for users. The platform will combine the specific standardized process for functional operation, improve the awareness and skill level of the exercisers for space Internet security, and achieve the purpose of integrating theory and practice.

5 SPIDERLAND

5.1 Overview

Based on the overall architecture of Space Spider, we have developed an open software platform, Spiderland, to provide an experimental platform for practitioners and researchers of space Internet applications and security, as well as interested people. The tools carried by the platform cover every link and multiple aspects of the whole life cycle of the space Internet. According to users' different identities and purposes, the software can be divided into three categories: scientific research software, business software, and application software. The scientific research software was the space Internet simulation software, which included the physical layer, Networking layer, and solution layer, such as STK, NS-3, GMAT, etc. The business software is satellite manufacturing, satellite mission management, satellite data management, situation display software, etc. The application software includes emergency rescue software, logistics software, remote sensing software, etc.

On the other hand, it also provides an experimental environment for network security researchers. The space Internet application and simulation software have become the target objects of our network attack and defense experiments. At this time, this software has become our target and can also be divided into scientific research target, business target, and application target. Researchers could carry out attack and defense experiments on software through reverse engineering, vulnerability, and penetration test, to discover software vulnerability and improve defense ability.

It is worth noting that Spiderland is not the only software that is our target. The effect can be seen in the simulation software through the combination of virtual and real scene simulation. For example, when we use high-power jamming equipment to interfere with satellite telemetry, remote-control signals, and other hard-kill attack means, we can observe the satellite interference situation in the space Internet business software and respond in time.

5.2 Platform architecture

Spiderland adopts the cloud native and micro-service architecture to ensure the platform's high availability, scalability, and performance. As shown in figure 3, in the system architecture design, the hierarchical design method based on the underlying interface,

resource data, and application services is adopted to ensure the flexibility and efficiency of the system design, as well as the reliability and stability of the system. The application layer provides users with various services and scenarios to realize virtual and real scene simulation, task planning, task guidance, visualization situation, efficiency evaluation, platform maintenance and management, and other application services. The middle layer connects the application layer to the infrastructure layer. It is a layer that links the previous and the next. It uses the resources provided by the infrastructure layer to provide services for application layer users, including virtualization services, network services, and mirroring services. It provides operating system images, virtual security devices, virtual network device resources and physical target access for the platform, and content support services for scene simulation creation. Through API interface calls, it provides data calling services for upper-layer business applications, including API interfaces such as scenarios, images, tools, and data collection.

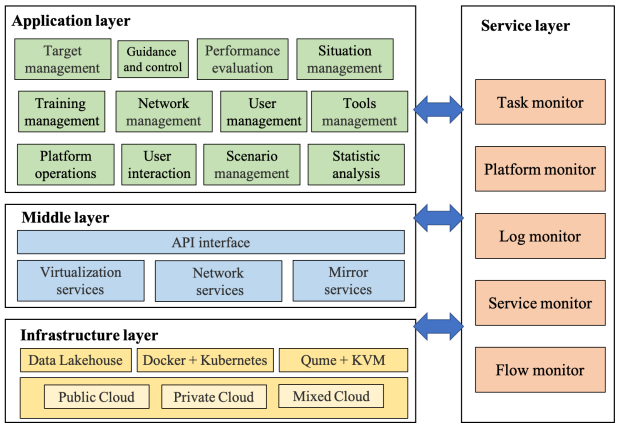

Figure 3: Architecture of Spiderland

The infrastructure layer provides required computing and data storage resources for the middle layer and pools resources through virtualization technology to achieve on-demand resource allocation and rapid deployment. It mainly uses server virtualization and application virtualization. In particular, to achieve the unified arrangement, management, and scheduling of Docker containers, we use the distributed architecture K8S based on Docker container technology. Spiderland can be deployed in scenarios and supports public clouds, private clouds, mixed clouds, and Linux operating systems.

In addition, to efficiently provide data resources, we adopt the data architecture of lake warehouse integration and severless data computing engine to store RDB, Kafka, HDFS, EOS, FTP, and other data forms on the cloud platform (data lake) to achieve near-real-time incremental update. Finally, the service layer is vertical and exists to manage better and maintain the infrastructure, middle, and application layers. This layer mainly monitors tasks, platforms, logs, services, and traffic.

6 CONCLUSION

This paper begins with an introduction to the social, economic, and strategic implications of the space Internet, followed by an explanation of its security risks. To defend against the security risks faced by the space Internet, we propose Space Spider, a hyper large scientific infrastructure based on digital twin for the space Internet, and introduce its core concept and technical framework. Finally, Spiderland, an open experimental platform for space Internet, is introduced.

REFERENCES

[1] Huan Cao, Lili Wu, Yue Chen, Yongtao Su, Zhengchao Lei, and Chunping Zhao. 2020. Analysis on the security of satellite internet. In *China Cyber Security Annual Conference*. Springer, Singapore, 193–205.

[2] Nan Cheng, Wei Quan, Weisen Shi, Huaqing Wu, Qiang Ye, Haibo Zhou, Weihua Zhuang, Xuemin Shen, and Bo Bai. 2020. A comprehensive simulation platform for space-air-ground integrated network. *IEEE Wireless Communications* 27, 1 (2020), 178–185.

[3] Jianli Du, Xiangxu Lei, and Jizhang Sang. 2019. A space surveillance satellite for cataloging high-altitude small debris. *Acta Astronautica* 157 (2019), 268–275.

[4] Giacomo Giuliari, Tobias Klenze, Markus Legner, David Basin, Adrian Perrig, and Ankit Singla. 2020. Internet backbones in space. *ACM SIGCOMM Computer Communication Review* 50, 1 (2020), 25–37.

[5] Mark Handley. 2018. Delay is not an option: Low latency routing in space. In *Proceedings of the 17th ACM Workshop on Hot Topics in Networks*. 85–91.

[6] Quan Hong, Yang Zhao, Jian Chang, Yuxin Du, Jun Li, and Lidong Zhai. 2022. Shock Trap: An active defense architecture based on trap vulnerabilities. In *2022 7th IEEE International Conference on Data Science in Cyberspace (DSC)*. 24–31. https://doi.org/10.1109/DSC55868.2022.00011

[7] Fenghua Li, Linjie Zhang, Mingyue Lu, Kui Geng, and Yunchuan Guo. 2020. Research on Space-Ground Network Security Guarantee Technology. *Space-Integrated-Ground Information Networks* 1, 1 (2020), 17–25.

[8] Le-Bao Li, Ming-Xiang Li, Lian-Xiang Jiang, Da-Yi Wang, Feng Zhan, and Tao Sheng. 2019. Angular rate estimation and damping control of satellite with magnetometer data. *Optik* 180 (2019), 1049–1055.

[9] Jiajia Liu, Yongpeng Shi, Zubair Md Fadlullah, and Nei Kato. 2018. Space-air-ground integrated network: A survey. *IEEE Communications Surveys & Tutorials* 20, 4 (2018), 2714–2741.

[10] Mengjie Liu, Yongqiang Gui, Jian Li, and Hancheng Lu. 2020. Large-scale small satellite network simulator: Design and evaluation. In *2020 3rd International Conference on Hot Information-Centric Networking (HotICN)*. IEEE, 194–199.

[11] Ruyue Liu, Jun Li, Lvyang Zhang, and Lidong Zhai. 2022. *POSTER: SpaceSpider: A Hyper Large Scientific Infrastructure For The Space Internet.* Technical Report. EasyChair.

[12] Zhong Ma, Yuejiao Wang, Yidai Yang, Zhuping Wang, Lei Tang, and Stephen Ackland. 2018. Reinforcement learning-based satellite attitude stabilization method for non-cooperative target capturing. *Sensors* 18, 12 (2018), 4331.

[13] Z. Mao, L. Zhou, and Y. Chen. 2020. A Satellite Communication Simulation System Research Based on HLA and MDIS. In *CSAE 2020: The 4th International Conference on Computer Science and Application Engineering*.

[14] Wittawat Tapsawat, Teerawat Sangpet, and Suwat Kuntanapreeda. 2018. Development of a hardware-in-loop attitude control simulator for a CubeSat satellite. In *IOP Conference Series: Materials Science and Engineering*, Vol. 297. IOP Publishing, 012010.

[15] Minghui Tian, Yaqing Wang, Lu Wang, and Xiaojing Xu. 2020. Ground target locating based on direction determination in satellite-borne. In *IET International Radar Conference (IET IRC 2020)*, Vol. 2020. IET, 1498–1502.

[16] Yanjun Yan, Guangjie Han, and Huihui Xu. 2019. A survey on secure routing protocols for satellite network. *Journal of Network and Computer Applications* 145 (2019), 102415.

[17] Lingcui Zhang, Yaobing Xu, Fenghua Li, Liang Fang, Yunchuan Guo, and Zifu Li. 2021. Dynamic security-empowering architecture for space-ground integration information network. *Journal on Communications* 42, 9 (2021), 87–95.

[18] H Zhu, H Wu, H Zhao, et al. 2019. Efficient authentication scheme for double-layer satellite network. *J. Commun* 40, 3 (2019), 1–9.