Survey on Security for Non-Terrestrial Networks

Seungbin Lee and Jiyoon Kim

Gyeongsang National University, Jinju, Republic of Korea

Received: October 07, 2024; Revised: November 11, 2024; Accepted: December 13, 2024; Published: December 26, 2024

Abstract

Non-terrestrial networks (NTN) are studied in a way that goes beyond the environmental limitations of existing terrestrial networks. In particular, it ensures connectivity in remote areas, rural areas, and areas where communication infrastructure is insufficient.

NTN leverages state-of-the-art space and aviation platforms to provide highly versatile services in domains such as IoT and disaster management. These NTNs are the cornerstone of next-generation communication systems, and at the same time, they are likely to address gaps in the connectivity of communications. In this paper, we examine the latest trends related to the security of NTN, and analyze its network-specific characteristics, methodologies, and challenges. Integrating NTN with the ground infrastructure creates security challenges such as seamless handover management between satellites and ground systems, cyber threats from quantum computers, and development of encryption technologies for IoT environments with limited resources. To address these challenges, this study categorizes NTN security requirements into security requirements that apply to all network operations and security requirements for the inherent vulnerabilities of NTN. According to the analysis of NTN, it highlights the need for Post Quantum encryption algorithm, robust handover security protocol, and lightweight encryption method suitable for the dynamic and resource-limited nature of NTN. Advanced technologies such as AI-based threat detection, blockchain-based mechanisms for data integrity, and adaptive security frameworks are showing the possibility of secure and scalable NTN communication. This paper raises recommendations for the secure integration of NTN with ground network based on the results of a recent comprehensive study. This survey provides direction to aid in the development of standardized security protocol and at the same time provide NTN future oriented communication solution. Addressing these challenges will show the potential of NTN as a key component of the global communication infrastructure in the coming era.

Keywords: Non-Terrestrial Networks, Security, Requirement.

1 Introduction

Advances in wireless communication technology are leading the transition of a new communication paradigm beyond 5G networks. Existing ground networks have shown limitations in providing stable connections in environments where communication connections are difficult or limited, such as at sea, mountains, and air. NTN is emerging as an innovative alternative to solving these problems. Leveraging advanced technologies such as satellite technology, high-altitude platforms, and aviation-based systems, NTN provides connectivity to areas such as isolated islands or rugged mountainous terrain, where communication was not possible in the past. These technologies do not just expand communication coverage, they simultaneously improve mobility and stability, and enable reliable connections in various communication scenarios [1-3].

The continuous development of NTN provides several advantages such as network coverage expansion, data processing capacity increase, and capacity increase. However, with these developments, new security challenges and challenges are also emerging. NTN infrastructure operates dynamically in a wide range of

DOI:https://doi.org/10.56801/rebicte.v10i.196

areas from low-orbit (LEO) to geostationary-orbit (GEO), and these characteristics lead to vulnerabilities such as signal blocking, unauthorized access, and cyberattacks on non-terrestrial components. In addition, NTN causes problems that cannot be adequately addressed by existing terrestrial network security frameworks due to high latency, frequent network topology changes, and complex data transmission paths. Therefore, the development of more robust and efficient authentication and security mechanisms is essential to protect network infrastructure and user data [4].

This study examines the key roles that NTN play in the modern communication environment, focusing in particular on New Radio Non-Terrestrial Networks (NR-NTN) and Internet of Things Non-Terrestrial Networks (IoT-NTN). In addition, we analyze two main payload architectures designed to optimize resource allocation and ensure a reliable connection in NTN. This classifies the requirements for NTN security and suggests practical applicable security strategies. In addition, we also discuss future research directions to address the problems posed by advanced technologies [5,6].

NTN faces unique limitations and limitations in achieving the level of security on par with existing ground networks due to its heavy dependence on space and aviation-based components. For this reason, it is imperative to redefine NTN-specific security requirements and to develop customized security solutions based on them. To address this gap, this paper presents a comprehensive and systematic framework for NTN security by synthesizing existing research results. This framework is divided into two categories. The first is the basic security requirements for network operation and service delivery, and the second is the NTN-specific security requirements to address the inherent vulnerabilities arising from ground technologies.

2 Non-Terrestrial Networks

NTN is attracting attention as an important solution in environments where it is difficult to provide a stable connection with the existing communication infrastructure, such as rural, maritime, and air regions. Existing ground networks have shown limitations in providing continuous and stable services in areas with limited access and are also struggling to respond quickly to natural or emergency situations. Therefore, NTN supports wide coverage and high mobility and solves these problems through communication systems that operate independently beyond geographic constraints.

NTN utilizes satellites and high-altitude platforms to provide reliable connectivity even in areas with low communication access, such as islands, mountainous areas, seas, and the air. These technologies enable better network integration through interaction with existing communication infrastructure and demonstrate the potential for development into a hyperconnected society. Furthermore, NTN has the potential to accelerate innovation in various fields such as smart agriculture, telemedicine, and IoT-based services. This is expected to create new values across society and further promote digital transformation.

2.1 Overview

NTN integrates various platforms to provide a wide range of connections. These public platforms are complementarily designed to overcome environmental or situational constraints and form a communication network. The NTN platform is designed based on an altitude and network topology optimized to meet specific requirements. For example, the NTN platform includes the ability to reduce the latency of high-speed data or support emergency situations in the surrounding area. Figure 1 shows the main platforms and roles of NTN.

- Low Earth Orbit (LEO): LEO satellites are positioned at altitudes ranging from 200 to 2,000 kilometers above Earth's surface. LEO satellites provide low latency and high-speed communication. Technological advancements have made LEO satellites cost-effective and scalable. Extensive deployment across various applications is possible with LEO satellites.

- Medium Earth Orbit (MEO): MEO satellites operating at altitudes of 2,000 to 35,786 kilometers achieve a balance between latency and coverage. Navigation systems such as GPS and Galileo require consistent and precise positioning, creating an environment favoring MEO satellites.

- Geostationary Orbit (GEO): GEO satellites positioned at approximately 35,786 kilometers maintain a fixed position relative to Earth's surface. A fixed position enables stable coverage for broadcasting, communications, and weather monitoring applications.

- High-Altitude Platform Stations (HAPS): HAPS deployed at altitudes of 17 to 22 kilometers function as effective connectivity solutions in regions where conventional ground infrastructure is either unfeasible or prohibitively expensive. HAPS also deliver targeted communication services to areas with limited coverage.

- Unmanned Aerial Systems (UAS): Flexible and mobile platforms offer ideal deployment options in disaster-affected or remote areas. UAS rapidly establish communication links, ensuring uninterrupted connectivity during emergencies or in difficult-to-access regions.

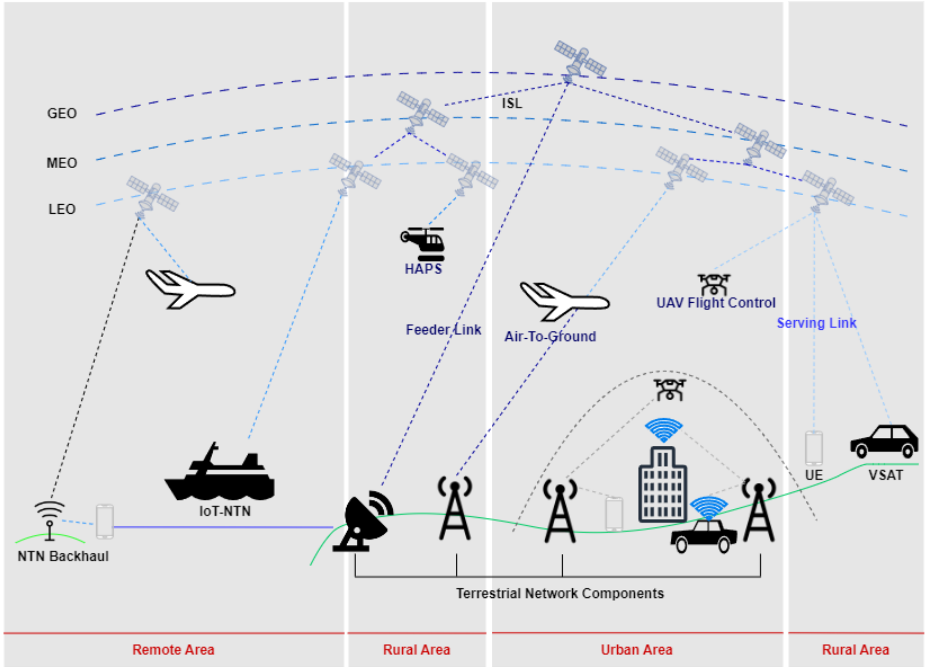

Figure 1. Non-Terrestrial Network Platform

2.2 Payload Architectures in NTN

The payload architecture is a key component of NTN and plays an important role in the efficiency, safety, and overall performance of communication systems. This architecture is divided into Transparent payload and Regenerative payload. These architectures perform key tasks such as data relay and processing transmission and support complementary connections between ground and non-ground platforms. Through this, NTN provides stable and smooth communication services in complex geographic environments. Each type of payload architecture is designed based on its unique characteristics and advantages and is selected in an appropriate manner according to the requirements of a specific application field and operating environment [4,7].

2.2.1 Transparent Payloads

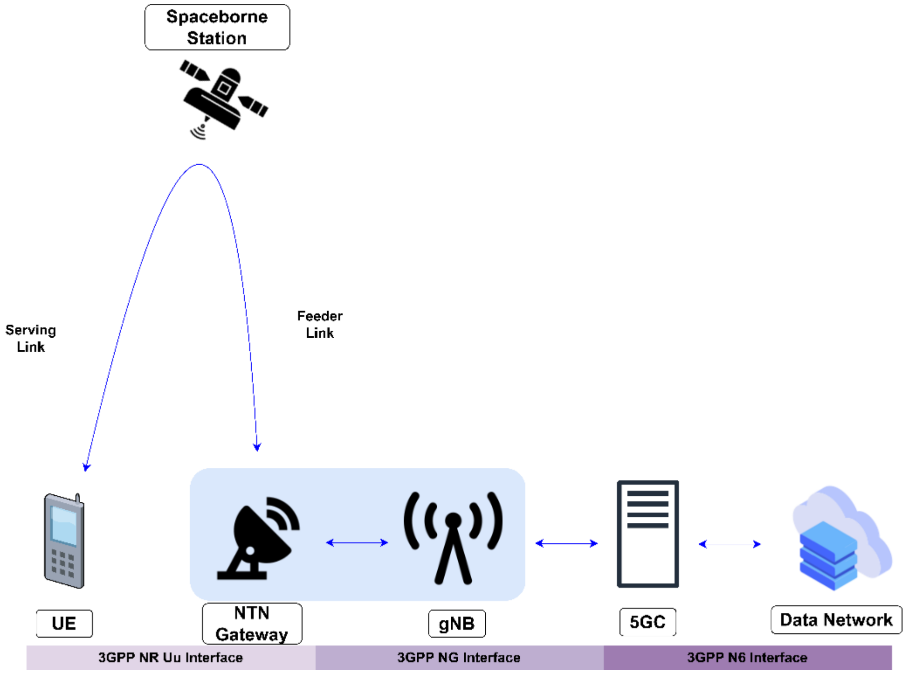

Figure 2. Transparent Payloads Architecture

Figure 2 illustrates Transparent payloads Architecture. Transparent payloads, commonly referred to as "bent-pipe" systems, simply relay signals without modifying data. They amplify incoming signals and deliver them to destinations, enabling low-latency communication with minimal processing. This simple design provides energy efficiency and cost-effectiveness, especially useful for platforms with limited power resources. In addition, Transparent payloads are highly compatible with existing ground network infrastructure and can be easily utilized without complex coordination for integration and deployment [8]. However, since Transparent payload does not modify or process transmitted data, interference or noise included in the existing signal may be relayed as it is, and thus signal quality may be deteriorated. In addition, major functions such as signal decoding, error correction, and protocol management depend entirely on the ground station. This dependence may lead to performance degradation in remote areas or in environments where ground infrastructure is not available, such as in emergency situations.

Transparent payloads are most suitable for applications that prioritize simplicity, cost efficiency, and low latency. Common use cases include television broadcasting, basic connectivity in regions with established infrastructure, and temporary communication solutions during emergencies. Their low operational complexity and energy efficiency make them an excellent choice for environments supported by reliable ground systems.

2.2.2 Regenerative Payloads

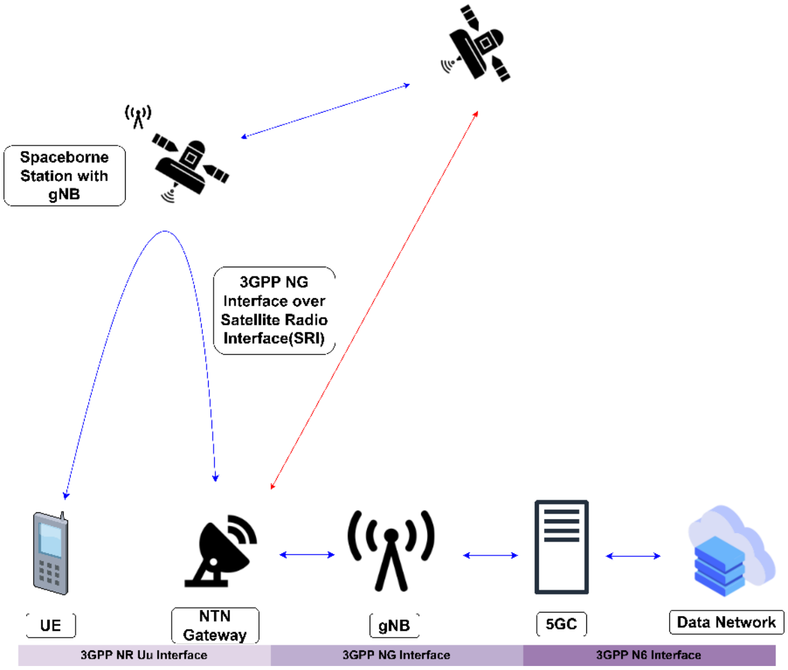

Figure 3. Regenerative Payloads Architecture

Figure 3 illustrates Regenerative payloads Architecture. Regenerative payloads integrate on-board processing functions to decode, process, and re-encode signals before retransmission, which are different from Transparent payloads. This function improves signal quality by reducing noise and correcting errors. In addition, regenerative payloads can dynamically adapt to network conditions to optimize bandwidth utilization, prioritize important data streams, and perform protocol changes. Unlike Transparent payloads, they are effective for deploying in remote or communication-less connected areas due to low dependence of the ground station and are suitable for emergency and disaster situations [9]. The functions provided by regenerative payloads are essential in modern communication systems. It is suitable for intensive data tasks such as aggregating and filtering information in IoT networks. In real-time video streaming, where it is important to maintain data integrity and minimize errors, regenerative payloads show high performance. These onboard processing and encryption functions play an important role in fields such as industrial automation and defense that enhance operational security and safety.

However, the regenerative payload is more complex and requires a lot of development and operation costs. A static exchange heat management system is required to ensure power consumption and optimal performance, and latency may occur due to on-board processing, which may pose difficulties for applications that must ensure real-time performance.

2.2.3 Comparison between Transparent Payloads and Regenerative Payloads

Developed with a focus on simple design and cost-effectiveness, transparent payloads are evaluated as an appropriate choice for applications that need to operate within a limited budget while meeting basic communication requirements. On the other hand, playback payloads are optimized for advanced communication scenarios where data throughput is high or security is critical through the characteristics of higher performance, adaptability, and enhanced data integrity. As a result, the choice of these two payload architectures is based on various factors such as the application's latency tolerance, supportable infrastructure, and financial constraints.

In the future, it is expected that a hybrid system that combines the advantages of transparent and renewable payloads will provide an optimal solution for NTN deployment. Such a system can contribute to meeting the various and complex requirements of the global communication network while maintaining a balance between cost-effectiveness and performance. Hybrid systems encompass both data-intensive and budget-constrained applications that require high performance, with the potential to further improve the flexibility of communication networks. Table 1 shows the main differences between transparent and playback payloads, their respective functions, and representative use cases at a glance. Through this, a clear criterion for which situation each architecture is best suited is presented [8, 9].

Table 1. Comparison between Transparent Payloads and Regenerative Payloads

Feature	Transparent Payload	Regenerative Payload
Functionality	Simple signal relay without processing	On-board signal processing, including modulation and error correction
Latency	Low, as no processing is performed	Higher, due to on-board processing tasks
Complexity	Simple design and operation	Complex design requiring advanced hardware and software
Cost	Lower development and operational costs	Higher due to advanced processing capabilities
Power Consumption	Low energy requirements	High energy demand for processing tasks
Signal Quality	Relays data with existing noise and interference	Removes noise and corrects errors, improving quality
Reliance on Ground Systems	High, as all processing occurs at ground stations	Low, as most processing is handled on-board
Security	Limited, as data is relayed without encryption	Enhanced, with on-board encryption and processing
Adaptability	Limited to basic relaying tasks	Dynamically adjusts to changing network conditions
Applications	Suitable for low-cost, low-complexity scenarios	Ideal for advanced, high-density, and secure applications

2.3 Recent Studies

NTN is expected to play a key role in connecting remote locations and underserved areas. Prior to performing this role, NTN faces the unique security challenges it has. NTN has environmental characteristics such as high mobility, various platforms, and fluctuating latency, and it is difficult to apply these characteristics to existing security systems, resulting in security vulnerabilities.

In order to solve these security problems, a security system that takes into account the characteristic of NTN is needed. These security problems facing NTN include signal blocking, unauthorized access, and cyberattacks targeting non-terrestrial assets. In particular, it is essential to ensure safe communication even in areas where ground-based infrastructure is scarce and to maintain the stability and reliability of NTN operations to manage Doppler effects that may occur over long communication paths.

To enhance NTN security, recent research has developed security strategies targeting different communication layers. At the physical layer, anti-interference and anti-spoofing technologies are utilized to increase resilience from external interference. At the encryption layer, advanced technologies such as lightweight encryption protocols and quantum key distribution (QKD) are being applied to protect sensitive data. At the same time, new technologies such as AI, ML and blockchain are integrated into the security framework to further enhance NTN security by enabling real-time threat detection, secure handover, and data integrity verification. Standardization work also plays an important role in enhancing NTN security. The international organization, 3GPP, has established guidelines for integrating the security protocols of NTN and existing ground networks, ensuring interoperability and consistent security measures between networks. These standardization efforts not only facilitate the integration between NTN and ground networks, but also make important contributions to maintaining consistent security in the global communication environment.

This section introduces a variety of state-of-the-art studies that have been proposed to address the security challenges of NTN. This includes utilizing AI technology for real-time threat detection and introducing QKD to enhance data protection. These studies adopt a multifaceted and innovative approach to address the unique security challenges facing NTN. This approach plays a key role in building a reliable and reliable communication environment. In particular, with the growing use of NTN, efforts to achieve such goals as real-time threat detection, secure data transfer, and ensuring network integrity are becoming more important. These studies provide an essential security foundation for the next generation of communication systems and support the continuous development and safety of NTN.

Kumar et al. [11] propose a hybrid security scheme combining AI and blockchain to address the security threats faced by NTN, especially DoS attacks and data breaches. This study proposes a new approach to leverage blockchain technology to ensure data integrity and transparency, while also improving anomaly detection and decision-making process through AI. In particular, we introduce how to use smart contracts to form secure agreements. This approach provides important references for future network security architecture development.

Iqbal et al. [12] studied an AI approach combining Deep Reinforcement Learning (DRL) and anomaly detection techniques to optimize resource allocation and mitigate security threats such as spoofing in NTN. This study highlighted the importance of federated learning in enhancing privacy and advancing collaborative threat intelligence in NTN systems. Federated learning has been proposed as a promising technique to ensure the privacy of data in a distributed environment while maintaining the efficiency of model learning.

Dahouda et al. [13] proposed a machine learning approach to address security vulnerabilities that occur during handover in LEO satellite networks. In this study, seamless connectivity was ensured through fast cell transition using clustering and classification models. In particular, the Random Forest algorithm has been demonstrated to be effective in optimizing handover strategies and providing secure connectivity even in the dynamic topology of LEO. This study shows the potential of machine learning technology to simultaneously enhance security and connectivity in NTN environments.

Plastras et al. [14] proposed a lightweight encryption protocol and an adaptive resource allocation method as approaches to increase the power efficiency of IoT devices and maintain data integrity. This approach focuses on expanding the coverage of IoT networks by utilizing the support of satellites and unmanned aerial vehicles (UAVs) and ensuring security and reliability even in areas where existing communication infrastructure is not reachable. Through this, we presented the possibility that IoT technology can be applied more effectively in the global environment.

Saad et al. [15] reviewed the security features proposed in 3GPP releases 17 and 18 to address the security issues of NTN. The main contents include secure handover, data protection between networks, and delay reduction mechanisms, and emphasized that standardization plays an important role in ensuring interoperability and secure communication in hybrid systems.

Rinaldi et al. [16] proposed Regenerative payload, encryption protocol, and multiple connection technologies to cope with threats such as eavesdropping and signal interference. It also emphasized that AI-based real-time threat detection is emerging as a promising technology by integrating adaptive handover and blockchain technology.

Yahia et al. [17] analyzed that Free space Optical (FSO) communication of satellite-ground and aerial platform networks is vulnerable to eavesdropping and atmospheric interference. This study proposed ways to reduce the probability of secret interruption, alleviate the turbulence problem, and strengthen security in the physical layer.

Tedeschi et al. [18] categorized threats such as jamming and spoofing that may arise in satellite communications and emphasized the need for the introduction of quantum encryption and the design of a physical layer security framework to address them.

Ahmad et al. [19] analyzed policy discrepancies and data breaches occurring in the satellite-to-ground handover process through the case of Viasat cyberattacks. This study suggested the need for improved runtime security and advanced encryption technology to strengthen the security of handover.

3 Security Requirement for Non-Terrestrial Networks (NTN)

The role of NTNs is gradually expanding in areas where communication is difficult, especially remote locations and in underserved environments. Accordingly, the need to solve security problems has been raised importantly. NTN has different technical characteristics from existing terrestrial networks and is more affected by high mobility, propagation delays, and physical and cyber threats. Therefore, a systematic security framework that can maintain the confidentiality, integrity, and availability of data is required to cope with the complex and diversified environment of NTN.

In this section, the security requirements of NTN are presented in two ways. First, the general security standard applicable to all NTN operations, and second, the specific security requirements designed to address the problems inherent to NTN. These requirements provide the basis for enabling a stable and reliable design of NTN.

Recent studies have shown that the security requirements of NTN are as follows.

3.1 General Security Requirement

1. Data Confidentiality: Protection of transmitted data from unauthorized access through encryption techniques, such as lightweight cryptography or QKD.

2. Data Integrity: Prevention of unauthorized modifications to data during transmission, using cryptographic hash functions and integrity checks.

3. Authentication and Access Control: Verification of user and device identities through methods like multi-factor authentication and blockchain-based identity management.

4. Availability: Ensuring uninterrupted network services by mitigating threats such as jamming and denial-of-service attacks through redundancy and adaptive routing.

5. Interoperability: Seamless communication between NTN and terrestrial networks through standardized protocols and secure handover mechanisms.

6. Scalability: Handling an increasing number of devices and connections through scalable security protocols and adaptive resource management.

7. Low Latency: Reducing delays to support real-time applications by optimizing security protocols to minimize processing overhead.

3.2 NTN-specific Security Requirement

1. Handover Security: Protecting data and ensuring continuity during frequent handovers in high-mobility networks, especially for LEO satellite systems, using machine learning-based optimization strategies.

2. Quantum-Resistant Cryptography: Preparing for future quantum threats by adopting quantum-safe cryptographic methods and leveraging QKD for secure key exchange.

3. Physical Layer Security: Addressing vulnerabilities at the physical layer through techniques like artificial

noise generation, beamforming, and secrecy outage modeling.

4. Energy-Efficient Security: Developing lightweight encryption methods for low-power IoT devices in NTN environments to balance security and energy efficiency.

5. Anti-Jamming and Anti-Spoofing: Countering signal disruption and impersonation attacks with AI-driven detection systems and robust threat mitigation strategies.

6. Blockchain-Based Data Integrity: Using blockchain for immutable and transparent data sharing, ensuring secure consensus in decentralized NTN systems.

7. Adaptive Security Protocols: Designing security mechanisms that dynamically adjust to changing conditions, including mobility and latency variations.

8. Secure Multi-Connectivity: Enabling devices to connect to multiple NTN nodes simultaneously, reducing risks of single-point failures and enhancing network resilience.

9. Runtime Security Measures: Implementing real-time security frameworks to protect hybrid NTN-terrestrial networks against evolving threats.

10. Critical Infrastructure Protection: Securing NTN links used for defense, disaster recovery, and industrial IoT applications with advanced encryption and anomaly detection.

Figure 4 visually shows the interaction between the security requirements highlighted in the recent NTN study and the various methodologies.

The security requirements are divided into general security requirements applicable in various network environments, and the other is NTN security requirements designed to address the unique challenges of NTN. This figure helps to understand the NTN security framework by specifically explaining how the requirements are implemented and supported in each research methodology.

Table 2 contains the results of a comparative analysis of various methodologies and technologies designed to solve the major challenges facing NTN. Through a detailed explanation of the strengths and weaknesses of each approach and the practical applicability, it is possible to evaluate which technologies are suitable for a specific use case. Representative core technologies include AI-based resource management, blockchain-based security mechanism, and energy efficiency-focused lightweight encryption protocols.

In addition, this table highlights the need for a multi-faceted approach that combines effective solution methodologies such as high mobility, diverse platforms, fluctuating latency, and integration problems with ground networks, which are the major challenges of NTN. This approach plays an important role in meeting the specific security requirements of NTN by dealing with complex problems that are difficult to solve with a single technology.

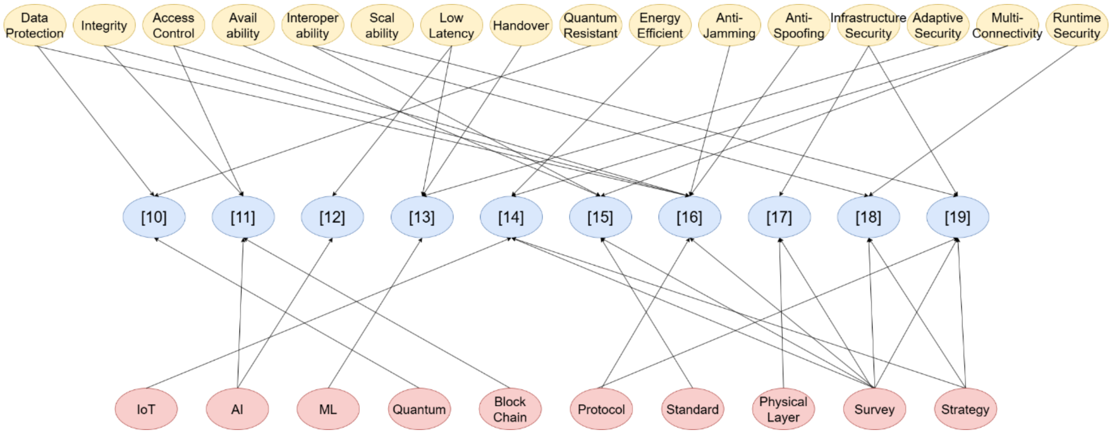

Figure 4. Derivation of Security Requirements from Recent Studies

Table 2. Recent Studies in NTN Security

Paper	Contribution	Methodology	Security Focus	Applications
Lauterbach et al. [10]	Quantum encryption; Secure satellite communication.	QKD protocols; Atmospheric effects.	Quantum-based Key distribution	Global secure communication.
Kumar et al. [11]	Blockchain framework; Distributed AI security.	Smart contracts; AI-driven anomaly detection.	Data integrity; Privacy preservation.	Dynamic NTN security; Blockchain-enabled.
Iqbal et al. [12]	AI for threat detection; Real-time NTN security.	Deep learning; Anomaly-based threat mitigation.	Anti-jamming; Anti-spoofing.	Threat mitigation in NTN nodes.
Dahouda et al. [13]	ML for handover; Optimized LEO satellite security.	Random forest; Clustering for handovers.	Secure handovers; Mobility resilience.	Mobility-intensive LEO security.
Plastras et al. [14]	Energy-efficient encryption; IoT focus.	Lightweight cryptography; Resource optimization.	Low-power secure communication.	IoT in remote/disaster zones.
Saad et al. [15]	3GPP Release 17/18; NTN-TN integration security.	Standards analysis; Interoperability focus.	Handover security; Protocol enhancements.	Hybrid NTN-TN seamless operation.
Rinaldi et al. [16]	Satellite security survey; Threat countermeasures.	Survey of threats and solutions.	Eavesdropping; Jamming prevention.	Defense and commercial satellite security.
Yahia et al. [17]	FSO security; Physical-layer security.	Secrecy outage modeling.	Optical link security; Physical-layer integrity.	High-throughput optical NTN services.
Tedeschi et al. [18]	Hybrid NTN-TN security; Runtime measures.	Case studies; Cyberattack analysis.	Hybrid network protection.	Critical infrastructure; Data sharing.
Ahmad et al. [19]	NTN architecture; Security for hybrid systems.	Adaptive mechanisms; Security enhancements.	Dynamic topology; Adaptive security.	Comprehensive NTN security strategies.

4 Conclusion

NTN supports applications such as IoT and disaster recovery and shows the potential of global communication systems by providing connections to remote locations and underserved areas. NTN is expected to be able to provide wider coverage, improved mobility, and stable service connectivity through integration with ground networks. However, in order to realize these benefits, the challenges of securing and maintaining the NTN infrastructure must be addressed. NTN has its unique characteristics of high mobility, variable latency, and easy exposure to physical and cyber threats. It is not effective to solve these problems with existing security systems. Therefore, security measures taking these unique characteristics into account are essential, and through this, the safety and reliability of NTN must be guaranteed.

Recent studies classify the security requirements of NTN into two main categories. The first is a general security requirement that deals with the basic principles applicable to all network environments. The three elements of security, such as authentication mechanisms to ensure the confidentiality, integrity, and availability of data, access control, and interoperability with ground networks, are included. In addition, scalability for efficient processing due to increased traffic is also considered an important element of the security framework. The second is the NTN security requirement that addresses the unique challenges that arise in the architecture and operating environment of NTN. It requires the implementation of a post-Quantum encryption algorithm to cope with the potential threats posed by the development of quantum computers and a handover security mechanism to address the security vulnerabilities that may arise during the handover process to maintain seamless connections in satellite systems.

To enhance the security of the physical layer, implementing technologies such as anti-interference mechanisms and signal blocking measures is crucial. These techniques play an essential role in ensuring the stability and dependability of NTNs. Furthermore, energy-efficient security protocols have gained prominence, especially in resource-constrained environments like IoT systems. These protocols aim to maintain data integrity while reducing power consumption, taking into account the limited capacities of such devices. Blockchain technology, meanwhile, is emerging as a promising approach to bolstering data integrity and transparency within distributed networks. Dynamic networks such as NTNs frequently experience fluctuating conditions, necessitating adaptive security frameworks to effectively manage these changes. These frameworks are designed to provide flexible and responsive mechanisms for mitigating threats and adapting to evolving scenarios. However, significant challenges remain. For instance, time-sensitive applications, including autonomous vehicles and industrial IoT systems, must balance the competing demands of low latency and robust security—an ongoing technical hurdle.

Additionally, free-space optical (FSO) communication systems face vulnerabilities like atmospheric interference and misalignment, which must be addressed to improve their overall performance. Tackling these challenges is critical to achieving a stable and reliable communication environment.

Measures such as beamforming and secure outage modeling are required to solve this problem. In addition, it is necessary to develop an efficient mobility management protocol to prevent disruptions and security dementia that may occur during handover occurring in satellite constellation.

In summary, NTNs represent an innovative turning point in communication technology and have the potential to expand global connectivity and accessibility unprecedentedly. However, the success or failure of NTN depends on effectively addressing complex security challenges. By combining common security strategies with NTN-specific security approaches, and actively researching and applying new technologies, NTN can secure the resilience and reliability required for next-generation communication networks. In addition, collaboration among academic researchers, industry leaders, and standardization organizations serves as a key factor in the development of robust security frameworks. As NTN continues to develop, it is expected to provide secure and reliable communication in an accelerated world of digitalization and to redefine the global communication environment.

Funding Details

This work was supported by the National Research Foundation of Korea (NRF) grant funded by the Korea government (MSIT) (No. RS-2023-00210767).

Disclosure Statement

The author declares that (s)he has no relevant or material financial interests that relate to the research described in this paper.

Notes on Contributors

Seungbin Lee: He is currently an undergraduate student at Gyeongsang National University. His current research interests are 5G/6G and formal security analysis.

Jiyoon Kim: Received the B.S., M.S. and Ph.D. degrees in information security from Soonchunhyang University, Asan, Republic of Korea, in 2017, 2019, and 2022, respectively. He was a Senior Researcher at Kookmin University, Seoul, Republic of Korea. He is currently working as an Assistant Professor with the Department of Computer Science and Engineering, Gyeongsang National University, Jinju, Republic of Korea. His current research interests include 6G security, formal security analysis, protocol design and optimization.

References

[1] M. Saad, M. Tariq, M. Kahn, and D. Kim, "Non-Terrestrial Networks: An Overview of 3GPP Release 17 & 18," IEEE Internet of Things Magazine, vol. 7, pp. 20–26, Jan. 2024. doi: 10.1109/IOTM.001.2300154.

[2] G. Masini, P. Reininger, M. Jaafari, A. Veseley, N. Chuberre, B. Baudry, and J. Houssin, "5G meets satellite: Non-terrestrial network architecture and 3GPP," International Journal of Satellite Communications and Networking, vol. 41, pp. 249–261, Aug. 2022. doi:10.1002/sat.1456.

[3] S. Chen, Y. Liang, S. Sun, S. Kang, W. Cheng, and M. Peng, "Vision, Requirements, and Technology Trend of 6G - How to Tackle the Challenges of System Coverage, Capacity, User Data-rate and Movement Speed," IEEE Wireless Communications, vol. 27, pp. 218–228, Feb. 2020. doi:10.1109/MWC.001.1900333

[4] M. Giordani and M. Zorzi, "Non-Terrestrial Networks in the 6G Era: Challenges and Opportunities," IEEE Network, vol. 35, pp. 244–251, Dec. 2020. doi: 10.1109/MNET.011.2000493

[5] Y. Zhang, W. Saad, M. Bennis, M. Debbah, and A. Hjørungnes, "5G-Advanced Towards 6G: Past, Present, and Future," IEEE Communications Surveys & Tutorials, vol. 25, no. 2, pp. 1403-1437, 2nd Quarter 2023.

[6] W. Cui, X. Feng, Z. Wang, and C. Fan, "Inter-Satellite Link Prediction with Supervised Learning: An Application in Polar Orbits," Aerospace, vol. 11, no. 7, 2023.

[7] B. Di, H. Zhang, L. Song, Y. Li, and G. Y. Li, "Evolution of Non-Terrestrial Networks From 5G to 6G: A Survey," IEEE Open Journal of Vehicular Technology, vol. 1, pp. 128-141, 2020.

[8] M. Rihan and T. Düe and M.A. Vakilifard and D. Wübben, and A. Dekorsy, "RAN Functional Split Options for Integrated Terrestrial and Non-Terrestrial 6G Networks," Proc. of the 2023 11th International Japan-Africa Conference on Electronics, Communications, and Computations (JAC-ECC'23), Alexandria, Egypt, Dec. 2023.

[9] O.B. Yahia, Z. Garroussi, B. Sansò, J.-F. Frigon, S. Martel, A. Lesage-Landry, G.K. Kurt, "A Scalable Architecture for Future Regenerative Satellite Payloads," arXiv:2407.06075, July 2024.

[10] F. Lauterbach, M. Vanëk, M. Mehic, and M. Voznak, "A Study on Quantum Key Distribution Satellite Communications," Proc. of the 2023 15th International Congress on Ultra Modern Telecommunications and Control Systems and Workshops (ICUMT'23), Ghent, Belgium, Oct. 2023.

[11] P. Kumar, R. Kumar, A.K.M. N. Islam, S. Garg, G. Kaddoum, Z. Han, "Distributed AI and Blockchain for 6G-Assisted Terrestrial and Non-Terrestrial Networks: Challenges and Future Directions," IEEE Network, vol. 37, no. 2, pages: 70-77, Sept. 2023.

[12] A. Iqbal, M.-L. Tham, Y.J. Wong, A. Al-Habashna, G. Wainer, and Y.X. Zhu, "Empowering Non-Terrestrial Networks with Artificial Intelligence: A Survey," IEEE Access, vol.11, pp. 100986-101006, Sept. 2023.

[13] M.K. Dahouda, S. Jin, and I. Joe, "Machine Learning-Based Solutions for Handover Decisions in Non-Terrestrial Networks," Electronics, vol. 12, no. 8, pp. 1759:1-19, April. 2023.

[14] S. Plastras, D. Tsoumatidis, D.N. Skoutas, A. Rouskas, G. Kormentzas, and C. Skianis, "Non-Terrestrial Networks for Energy-Efficient Connectivity of Remote IoT Devices in the 6G Era: A Survey," vol. 24, no. 4, pages: 1227:1-40, Feb. 2024.

[15] M.M. Saad, M.A. Tariq, M.T.R. Kahn, and D. Kim, "Non-Terrestrial Networks: An Overview of 3GPP Release 17 & 18," IEEE Internet of Things Magazine, vol. 7, no. 1, Jan. 2024.

[16] F. Rinaldi, H.-L. Maattanen, J. Torsner, S. Pizzi, S. Andreev, and A. Iera, "Non-Terrestrial Networks in 5G & Beyond: A Survey," IEEE Access, vol. 8, pp.165178-165200, Sept. 2020.

[17] O.B. Yahia, E. Erdogan, G.K. Kurt, I. Altunbas, amd H. Yanikomeroglu, "Physical Layer Security Framework for Optical Non-Terrestrial Networks," Proc. of the 2021 28th International Conference on Telecommunications

(ICT'21), London, UK, June, 2021.

[18] P. Tedeschi, S. Sciancalepore, and R.D. Pietro, "Satellite-based communications security: A survey of threats, solutions, and research challenges," Computer Networks, vol. 216, pp. 109246:1-18, Oct. 2022.

[19] I. Ahmad, J. Suomalainen, P. Porambage, A. Gurtov, J. Huusko, and M. Höyhtyä, "Security of Satellite-Terrestrial Communications: Challenges and Potential Solutions," IEEE Access, vol.10, pp. 96038-96052, Sept. 2022.

Author's Biography

Seungbin Lee: He is currently an undergraduate student at Gyeongsang National University. His current research interests are 5G/6G and formal security analysis.

Jiyoon Kim: He is received the B.S., M.S. and Ph.D. degrees in information security from Soonchunhyang University, Asan, Republic of Korea, in 2017, 2019, and 2022, respectively. He was a Senior Researcher at Kookmin University, Seoul, Republic of Korea. He is currently working as an Assistant Professor with the Department of Computer Science and Engineering, Gyeongsang National University, Jinju, Republic of Korea. His current research interests include 6G security, formal security analysis, protocol design and optimization.