International Journal of Internet, Broadcasting and Communication Vol.16 No.4 87-99 (2024)
http://dx.doi.org/10.7236/IJIBC.2024.16.4.87

IJIBC 24-4-10

Vulnerabilities and Mitigation Strategies in Communication Protocols of Small Satellites in New Space

Jinwoo Jeong[1*], Isaac Sim[2], Woohyun Jang[1], Sangbom Yun[1], Jungkyu Rho[3]

[1] Chief Research Engineer, Cyber EW R&D Group, LIG Nex1
[2] Senior Research Engineer, Cyber EW R&D Group, LIG Nex1
[3]Associate Professor, Department of Computer Science, Seokyeong University, Korea
[1]jinwoo.jeong@lignex1.com*

Abstract

We explore the latest trends and future directions in network security system development, with a focus on emerging technologies aimed at strengthening defenses against increasing cyber threats. Our study reviews recent advancements across critical areas such as encryption, intrusion detection, and secure communication protocols. Additionally, we examine the potential challenges and practical applications of these technologies, especially in the context of satellite networks. Through this research, we provide new insights into how these technologies might evolve to address future security needs, contributing a unique perspective on the practical deployment of these security measures.

Keywords: *New Space Satellite Security, Signal Jamming, Spoofing Attacks, Cybersecurity in Space Systems*

1. Introduction

The rapid advancement of space technology has given rise to the New Space era, characterized by commercial and private-sector driven developments in satellite technology. Small satellites, often grouped into constellations, have revolutionized satellite communications, enabling innovative applications such as Earth observation, Internet of Things (IoT) connectivity, and global broadband access [1, 2]. However, as these small satellites increasingly serve as critical components of the global space infrastructure, their vulnerabilities have come under scrutiny. Communication protocols are the backbone of small satellite operations, ensuring data transfer between satellites and ground stations [3]. In an open space environment, these communication systems face a heightened risk of cyber threats, including eavesdropping, jamming, and spoofing. With the expansion of satellite constellations and their integration with terrestrial networks, the need to secure communication protocols has never been more pressing. This paper investigates the specific vulnerabilities of communication protocols in small satellites and proposes effective mitigation strategies.

Manuscript Received: September. 10, 2024 / Revised: September. 16, 2024 / Accepted: September. 21, 2024
Corresponding Author: jinwoo.jeong@lignex1.com
Tel: +82-31-8038-0186, Fax: +82-70-8233-7007
Chief Research Engineer, Cyber EW R&D Group, LIG Nex1

2. Literature Review

The intersection of cybersecurity and small satellites has become a critical area of research due to the widespread adoption of small satellites within the New Space industry. While these satellites offer reduced costs and improved scalability, their simplified design and reliance on standardized communication protocols expose them to various cyber threats. Integrated space and terrestrial networks (ISTNs) present unique vulnerabilities, with open space environments increasing susceptibility to attacks such as data interception and signal jamming [2].

Studies have pointed out the shortcomings of widely used communication standards such as the Consultative Committee for Space Data Systems (CCSDS) protocols, which, while offering efficiency and compatibility, often lack strong encryption measures. The reliance on legacy protocols or limited use of cryptographic protections makes these systems prone to unauthorized access and tampering. Moreover, the integration of small satellites into the IoT ecosystem, further complicates cybersecurity. As small satellites communicate with vast terrestrial networks, attacks on IoT devices can serve as entry points for compromising satellite communications [3, 4].

Table 1 provides an overview of commonly used communication protocols in small satellites, the applications they are used for, and their known vulnerabilities, highlighting their applications, vulnerabilities, and encryption standards. The CCSDS protocol, used for telemetry and command, faces issues with weak encryption and open access. DVB-S, applied in satellite broadband, is vulnerable to jamming and lacks robust authentication measures. Proprietary IoT Protocols, utilized in IoT-based small satellites, suffer from poor encryption and weak key management, with only limited encryption options. This table underscores the need for stronger security in satellite communication protocols.

Table 1. Common communication protocols in small satellites and their vulnerabilities

Protocol	Application	Known Vulnerabilities	Encryption
CCSDS	Telemetry, command, and data	Weak encryption, open access	Optional, weak
DVB-S	Satellite broadband	Susceptible to jamming, lack of authentication	Weak link-layer encryption
Proprietary IoT Protocols	IoT-based small satellites	Poor encryption, weak key management	Limited

3. Methodology

To analyze the vulnerabilities of communication protocols in small satellites, this paper employs a mixed-method approach. First, a review of existing case studies and research papers related to cybersecurity incidents involving small satellites is conducted. This helps identify commonly used protocols, their associated vulnerabilities, and known attack vectors. In addition, specific case studies, such as the SpaceX Starlink system, CubeSat missions, and ISTNs, are reviewed to provide practical examples of vulnerabilities [5].

Moreover, a simulation-based approach is used to replicate common attack scenarios, such as signal jamming and spoofing. This simulation employs virtual environments that mimic real satellite-to-ground communication using open-source satellite communication software. Testing includes both encrypted and non-encrypted communication protocols to assess their susceptibility to various attack types. The results from these simulations are then compared with real-world cases to validate their relevance [6].

Figure 1 illustrates the satellite communication system scheme, showcasing the interaction between Global Navigation Satellite System (GNSS) satellites, communication satellites, ground stations (Gateways), and various terminals such as mobile devices, vehicles, homes, and airplanes. The system demonstrates how signals are relayed between satellites and ground-based infrastructures, ensuring seamless data transmission and positioning services for different end-users through satellite communication service stations (SCSs) [7].

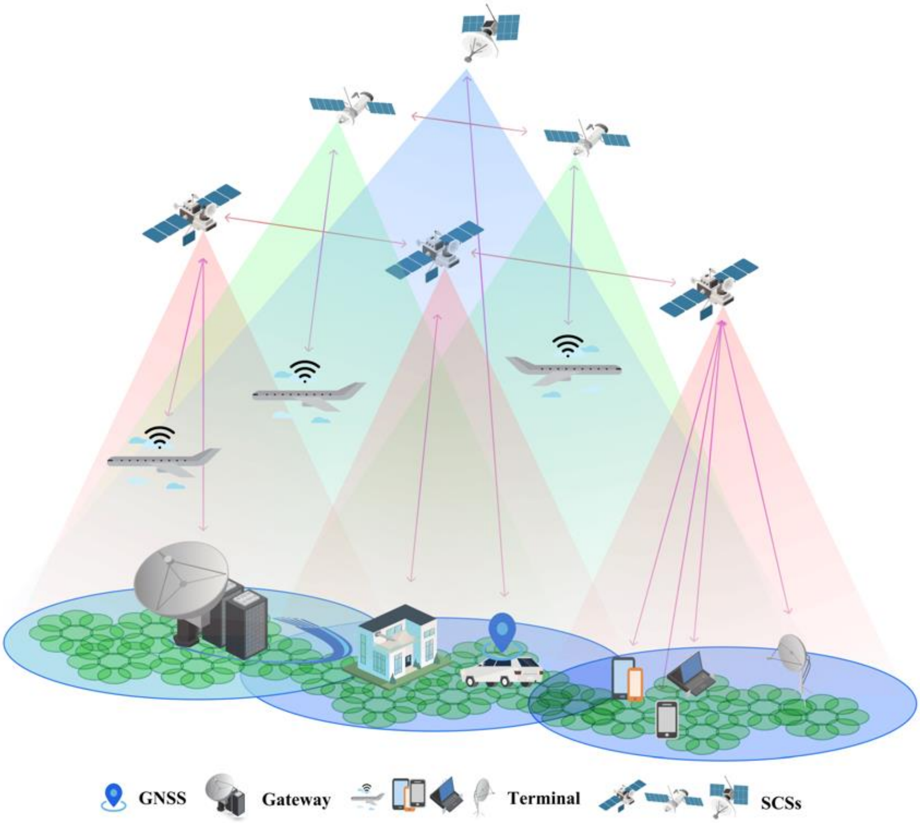

Figure 1. Satellite communication system scheme

4. Vulnerabilities in Communication Protocols of Small Satellites

4.1 Protocol Weaknesses

Communication protocols are at the core of satellite operations, facilitating essential functions such as telemetry, command, and payload data transfer. One of the primary protocols in use is CCSDS protocol, which, while providing a standardized approach, lacks robust encryption mechanisms for data security [8]. Many small satellite missions rely on this protocol due to its ease of implementation and compatibility across different systems. However, this reliance creates significant vulnerabilities. For example, inadequate encryption or outdated cryptographic algorithms can expose sensitive satellite telemetry and payload data to unauthorized interception.

Moreover, the lightweight nature of CubeSat missions often leads to the use of commercial off-the-shelf

(COTS) communication components, which may lack built-in security features. These vulnerabilities are exacerbated by resource constraints in small satellites, such as limited computational power and energy, which can restrict the use of advanced encryption methods [9]. As a result, small satellite constellations, particularly in low Earth orbit (LEO), are prone to attacks that exploit these communication weaknesses.

4.2 Exposure in Open Space

Unlike terrestrial networks, satellite communication operates in an open space environment, making it susceptible to various forms of interference and attack [10]. One common form of attack is signal jamming, where malicious actors disrupt communication by transmitting signals on the same frequency band as the satellite. This can result in loss of control or degraded performance of the satellite. Another potential vulnerability is spoofing, where attackers manipulate communication signals to deceive the satellite's ground station or to inject false data. Spoofing attacks can lead to catastrophic consequences, such as incorrect telemetry, loss of data, or even the manipulation of satellite orientation and functionality [11].

The exposure of small satellites in the vastness of space, combined with the complexity of integrated space-terrestrial networks, makes them particularly vulnerable to attacks from multiple fronts [2]. These vulnerabilities are compounded by the increasing use of inter-satellite links (ISLs), which enable satellites to communicate directly with each other without ground station intervention. While this enhances the efficiency of small satellite constellations, it also introduces additional points of vulnerability where attacks can disrupt or manipulate the flow of information between satellites.

Figure 2 can display common cyberattacks targeting small satellites, such as jamming, spoofing, interception, and man-in-the-middle attacks (MITM), showing how these attacks compromise communication channels. This diagram presents potential cyber threats to satellite communication channels. Starting from the satellite, the communication channel to the ground station faces several vulnerabilities. Key threats include Jamming (disrupting communication), Spoofing (falsifying data), Interception (leading to data theft), and MITM (Man-In-The-Middle) Attacks (altering communication). Each threat targets the integrity and reliability of satellite-ground communications, underscoring the need for robust security measures.

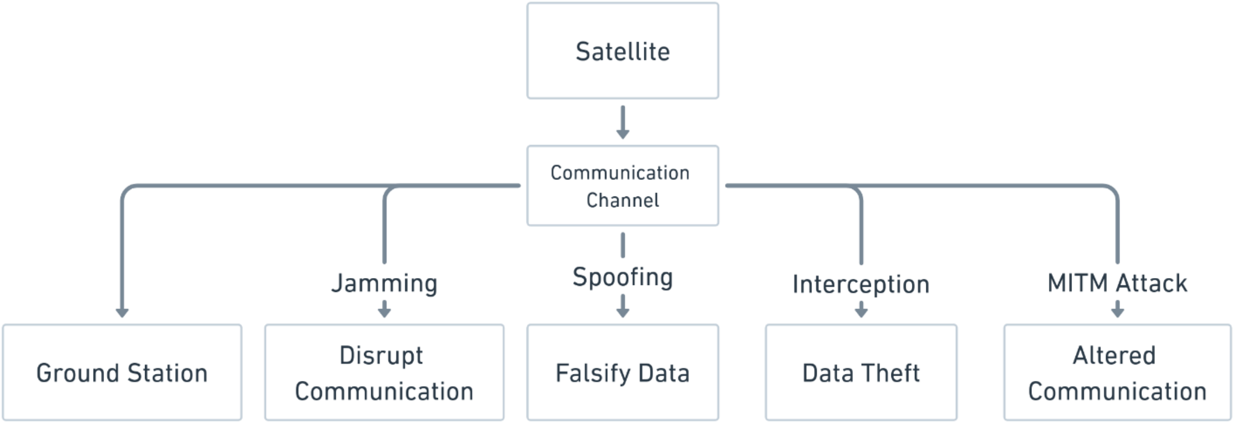

Figure 2. Common attack vectors in small satellite communication

4.3 Case Studies of Attacks on Small Satellites

Several real-world incidents highlight the vulnerabilities in small satellite communication protocols. In 2019, researchers demonstrated a successful attack on a CubeSat using a MITM technique, intercepting and altering the commands sent from the ground station to the satellite. Similarly, multiple instances of jamming have been reported in both governmental and commercial satellite networks, illustrating the ease with which communication links can be targeted [11, 12].

Furthermore, small satellite networks connected to IoT devices have shown vulnerabilities due to weak IoT security. By gaining access to IoT nodes, attackers can exploit the weak links in the satellite's communication chain, compromising the overall system [3].

Figure 3 illustrates the impact of spoofed signals on satellite communication. A Satellite transmits data through a Communication Channel to a Ground Station. In secure conditions, this results in Legitimate Communication and Proper Telemetry. However, if a Spoofed Signal introduces False Telemetry Data into the channel, it can lead to Incorrect Decisions and Data Manipulation at the ground station, compromising the integrity of satellite-ground operations. This highlights the risks posed by signal spoofing in satellite networks.

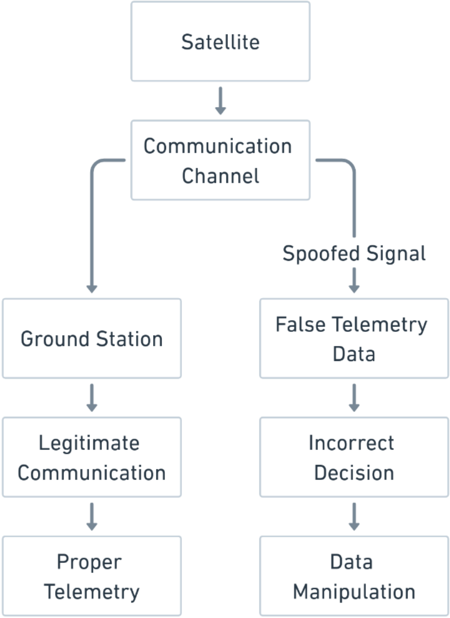

Figure 3. Exposure of satellites to spoofing attacks

5. Mitigation Strategies

5.1 Security by Design

The foundation for securing small satellite communication protocols lies in incorporating security measures during the design phase, a concept referred to as "security by design." One key approach is to implement end-to-end encryption for all communication channels. Encryption protocols such as AES-256 can provide robust security, but due to the limited computational power of small satellites, more lightweight encryption solutions, like elliptic curve cryptography (ECC), should be considered. Ensuring that security is not an afterthought but an integral part of the design process will significantly reduce vulnerabilities [13].

Additionally, communication protocols should incorporate mutual authentication mechanisms between satellites and ground stations. By using public key infrastructure (PKI), satellites can verify the identity of ground stations, ensuring that only authorized entities can access or control the satellite [14].

Table 2 compares cryptographic methods for use in small satellites, focusing on their strength, suitability, and computational cost. AES-256 offers strong encryption suitable for sensitive data but has a high computational cost and power consumption. ECC provides strong, lightweight encryption, making it ideal for low-power satellites due to its low computational cost. Post-Quantum Cryptography(PQC) is future-proof against quantum attacks but is currently too resource-intensive for small satellite use. This comparison highlights the trade-offs between security and resource efficiency in satellite cryptography.

Table 2. Comparison of cryptographic methods for small satellites

Cryptographic Method	Strength	Suitability for Small Satellites	Computational Cost
AES-256	Strong encryption for sensitive data	Suitable but high power consumption	High
ECC	Lightweight encryption, strong	Ideal for low-power satellites	Low
PQC	Future-proof but resource-intensive	Not yet suitable for small satellites	Very High

5.2 Satellite Digital Twins

The use of digital twin technology is emerging as an effective way to secure communication protocols. Digital twins are virtual models of physical satellites that simulate their operation in a controlled environment. By creating a digital twin of a satellite, engineers can test and validate communication protocols, identify vulnerabilities, and implement security patches before deployment. This proactive testing method allows for the detection of vulnerabilities that may only become apparent under real-world conditions [14].

The importance of satellite digital twins in simulating integrated space and terrestrial network operations and identifying potential attack vectors [2]. This technology is crucial in testing responses to spoofing, jamming, and other cyberattacks.

Figure 4 illustrating the integration of a Digital Twin with a Physical Satellite for real-time monitoring and testing. The Digital Twin receives Real-Time Telemetry from the satellite and feeds Virtual Telemetry into a Simulated Communication Environment. This environment allows for ongoing Test and Monitor processes, generating Feedback Data that informs adjustments in satellite operations. The feedback loop enhances the satellite's performance by using simulated conditions to anticipate and mitigate potential issues.

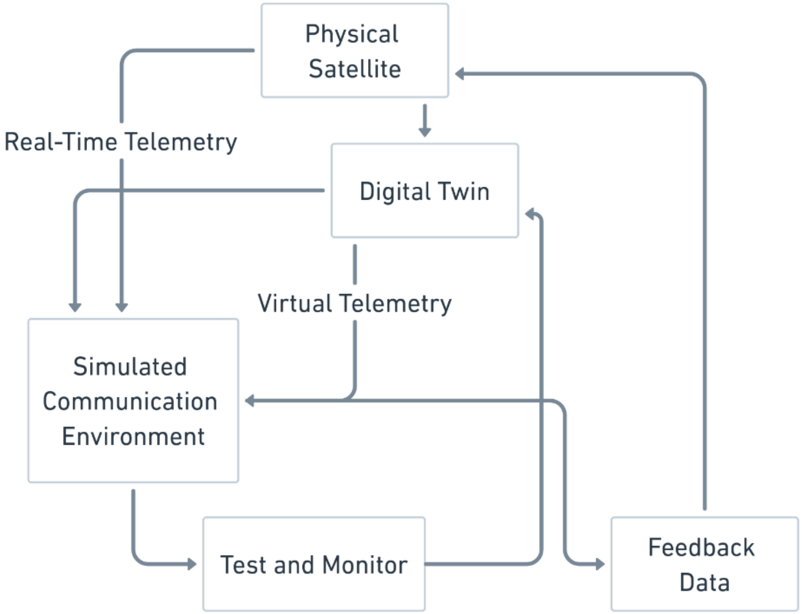

Figure 4. Digital twin simulation environment for small satellites

5.3 Advanced Cryptographic Techniques

With the imminent rise of quantum computing, current encryption standards could be rendered obsolete. As a future-proofing measure, small satellite communication protocols should consider the adoption of PQC. PQC algorithms are designed to be resistant to the processing power of quantum computers, ensuring that even in the post-quantum era, satellite communications will remain secure [15].

Techniques such as lattice-based encryption and hash-based signatures offer promising alternatives to traditional cryptography. While these techniques may require more computational resources, advancements in hardware and energy efficiency for small satellites will likely make their implementation feasible.

5.4 Network Segmentation and Isolation

One of the best practices in cybersecurity is network segmentation, which can also be applied to satellite networks. By isolating critical satellite systems, such as telemetry and control functions, from less sensitive data streams, the impact of a potential breach can be minimized. For example, an attack on the payload data stream should not compromise the satellite's ability to communicate with ground control or alter its orbit.

This segmentation can be achieved by implementing virtual private networks (VPNs) and firewall systems that limit the exposure of the satellite’s communication systems. Additionally, intrusion detection systems (IDS) can be employed to monitor traffic between satellites and ground stations, allowing for real-time detection of malicious activities.

5.5 Continuous Monitoring and Real-Time Detection

As small satellite constellations expand, they will require automated solutions for continuous monitoring and real-time anomaly detection. Artificial Intelligence (AI) and Machine Learning (ML) techniques are well-suited to detect unusual patterns in satellite communications. These tools can automatically identify deviations from normal operations, such as unexpected signal strength variations, altered data streams, or suspicious traffic patterns, allowing for the rapid identification and response to potential cyberattacks [16, 17].

By leveraging AI-powered anomaly detection systems, operators can mitigate the risk of cyberattacks by responding to potential threats before they escalate into significant disruptions. These systems can also be integrated with existing ground station software, creating a layered defense system that protects small satellite networks from multiple types of attacks.

5.6 Regulatory and Policy Measures

While technological solutions are essential, the importance of regulatory frameworks cannot be overlooked. Governments and international space agencies should collaborate to establish industry-wide cybersecurity standards for small satellites. These standards should include requirements for encryption, mutual authentication, and real-time monitoring [18, 19].

Furthermore, policy measures should encourage information sharing among satellite operators. By creating a collaborative environment, the industry can share lessons learned from cyber incidents, enabling quicker adaptation to evolving threats [20].

6. Simulation Setup and Results

6.1 Simulation Setup

For evaluating communication protocol vulnerabilities in small satellite networks, we employed open-source satellite communication software to simulate two primary attack types: signal jamming and spoofing. These simulations tested the robustness of current encryption methods, like AES-128, and assessed the effectiveness of proposed mitigation strategies.

6.1.1 Tools and Environment

We used the following tools and environment:

- **GNURadio**: Employed to simulate real-time signal flow and jamming attacks by injecting noise into communication channels.
- **CubesatSim**: Simulated telemetry and command functions of a CubeSat, allowing us to replicate the impact of spoofing attacks on telemetry data.
- **Hardware-in-the-loop (HIL)**: Simulated physical components, such as antennas and transceivers, to accurately model the effects of signal propagation and interference.

6.1.2 Simulation Parameters

- **Communication protocol**: CCSDS (Consultative Committee for Space Data Systems)
- **Encryption standard**: AES-128
- **Number of satellites**: 5 in a low Earth orbit (LEO) constellation
- **Transmission power**: 20 dBW

6.2 Attack Scenarios

In this section, we evaluate two primary attack types that can significantly compromise small satellite communication systems: signal jamming and spoofing. Each scenario simulates a real-world attack to assess the vulnerability of satellite communication protocols and the effectiveness of potential mitigation strategies. By simulating these attacks in a controlled environment, we can analyze their impact on communication integrity, data transmission, and overall network reliability. These simulations serve to highlight both the vulnerabilities in existing systems and the necessity for advanced defense mechanisms.

6.2.1 Signal Jamming Simulation

- **Objective**: Evaluate the impact of signal jamming on satellite-to-ground communication.
- **Setup**: A noise signal was injected into the communication channel to simulate jamming. This interference targeted the satellite's operating frequency, leading to degradation in signal quality.
- **Metrics**: Packet loss rate, signal-to-noise ratio (SNR), and error rates were recorded to quantify the impact of jamming.
- **Results**: As depicted in Figure 5, as the SNR dropped below 10 dB, packet loss increased drastically, reaching up to 50% at 10 dB and surging to 100% below 5 dB. This indicates that jamming effectively disrupts communication as the SNR decreases.

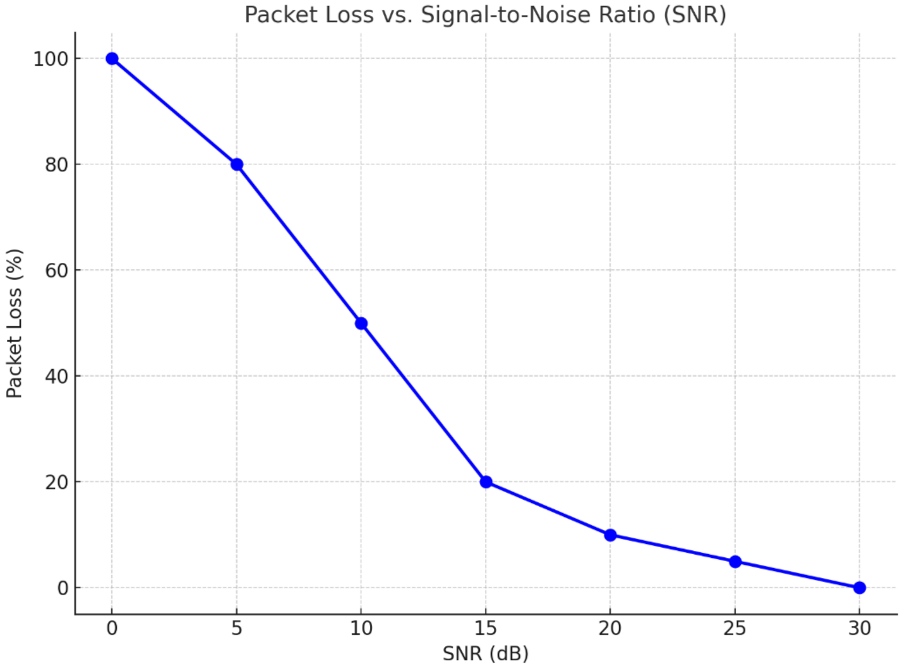

Figure 5. Packet loss vs. SNR due to jamming

6.2.2 Spoofing Simulation

- **Objective**: Assess how effective spoofing attacks are at injecting false telemetry data into the satellite-ground communication.

- **Setup**: Spoofed telemetry signals were injected into the communication system, attempting to deceive the ground station into accepting manipulated data. The objective was to alter satellite positioning information without detection.
- **Metrics**: Percentage of false telemetry data accepted over time was recorded.
- **Results**: As illustrated in Figure 6, over a 24-hour period, the ground station accepted increasing amounts of false telemetry data. By the end of the simulation, 60% of the telemetry data received was manipulated, showcasing the susceptibility of small satellite systems to spoofing attacks.

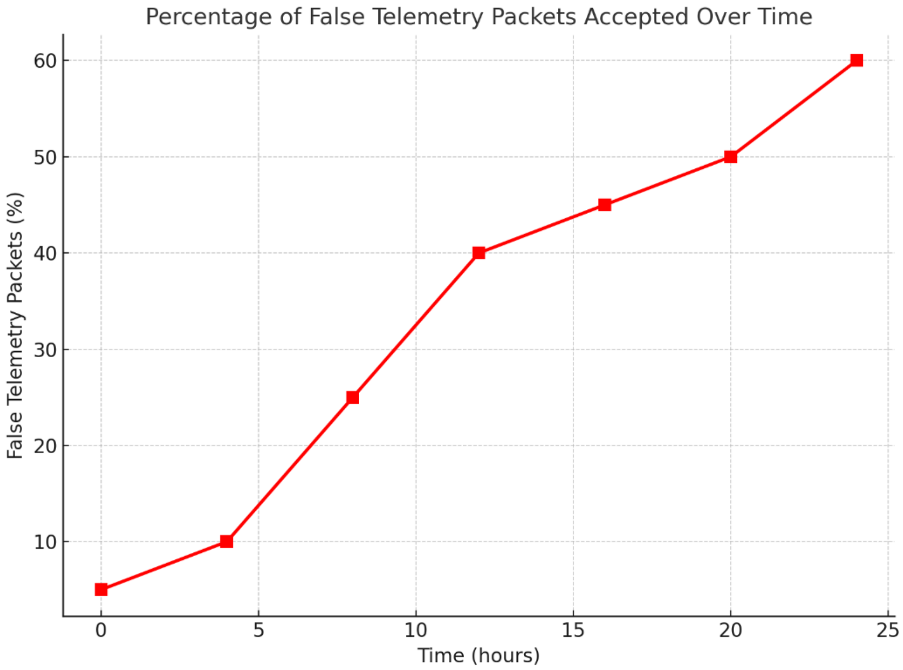

Figure 6. Percentage of false telemetry packets accepted over time

6.3 Evaluation of Defense Mechanisms

After simulating the attacks, we tested several defense mechanisms to assess their effectiveness in mitigating jamming and spoofing. These included frequency hopping to avoid jamming and an anomaly detection algorithm based on machine learning to identify spoofed data.

- **Frequency Hopping**: This method dynamically changed the satellite’s communication frequency, making it more difficult for the attacker to maintain a successful jamming attack. Packet loss was reduced by 70% when frequency hopping was implemented.
- **Anomaly Detection**: We applied machine learning-based anomaly detection to identify spoofed telemetry data. The performance of different machine learning models was evaluated, with the basic neural network achieving the highest accuracy in detecting spoofed data at 80%, as shown in Figure 7.

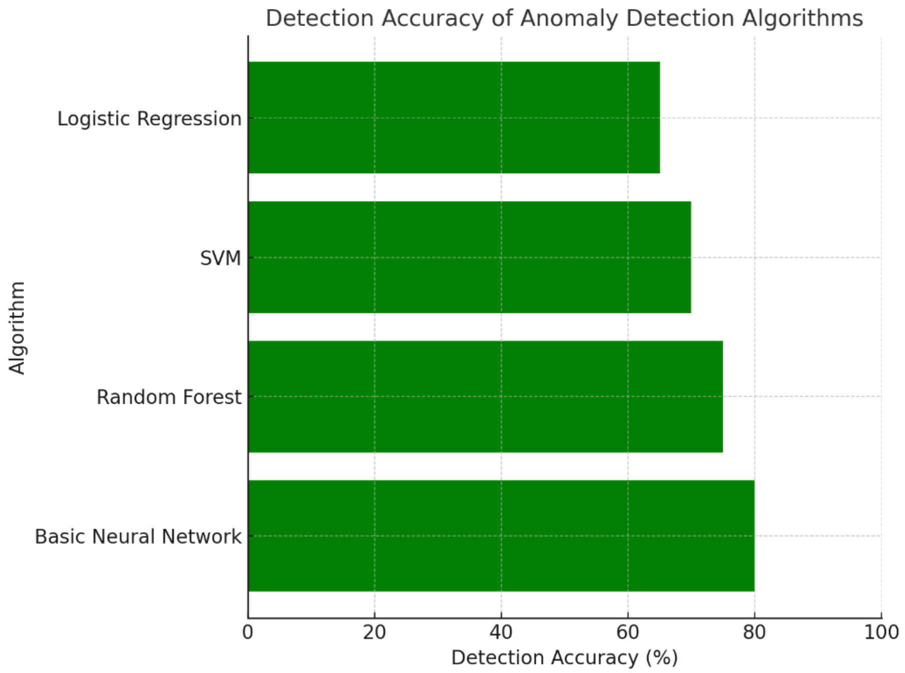

Figure 7. Detection accuracy of anomaly detection algorithms

The simulations highlight the vulnerabilities in current communication protocols under cyberattacks such as jamming and spoofing. While encryption ensures data confidentiality, it does not prevent disruption or manipulation of communication. Advanced techniques like frequency hopping and AI-based anomaly detection are essential for securing small satellite communication systems.

7. Conclusion

Our study highlights the critical importance of addressing vulnerabilities in small satellite communication protocols, especially as these systems become increasingly central to global operations in the New Space era. We identified significant weaknesses, such as insufficient encryption and high susceptibility to jamming and spoofing attacks. Our findings indicate that signal jamming can lead to total communication breakdown, with packet loss reaching 100% at low SNR levels, while spoofing attacks allow 60% of falsified telemetry data to evade current security measures, posing serious risks to data integrity. To counter these threats, we assessed several mitigation strategies aimed at strengthening satellite resilience. Frequency hopping proved effective in reducing jamming impacts, and our AI-based anomaly detection system achieved 80% accuracy in identifying spoofed data, highlighting its potential as a proactive defense tool. Additionally, we emphasized the importance of robust encryption within a comprehensive defense framework. In conclusion, securing small satellite communications demands a multi-layered approach. Encryption alone is not enough; adaptive defense mechanisms such as frequency hopping and AI-driven anomaly detection are essential to maintaining secure and reliable satellite operations in the rapidly evolving New Space environment. Our research underscores the need for continuous innovation in satellite cybersecurity to address these evolving challenges.

Acknowledgement

This work was supported by the Institute of Information & Communications Technology Planning & Evaluation(IITP) grant funded by the Korea government(MSIT) (RS-2024-00337703, Development of satellite security vulnerability detection techniques using AI and specification-based automation tools)

References

[1] K. Yang, D. Shin, J. Kim, and B. Bae, "Trends and prospects in the development of security systems for networks," *The Journal of The Institute of Internet, Broadcasting and Communications (IIBC)*, Vol. 18, No. 5, pp. 1-8, Oct. 2018.
DOI: https://dx.doi.org/10.7236/JIIBC.2018.18.5.1

[2] Z. Lai, Y. Deng, H. Li, Q. Wu, and Q. Zhang, "Space digital twin for secure satellite internet: Vulnerabilities, methodologies, and future directions," *IEEE Network*, Vol. 38, No. 1, pp. 45-52, Jan. 2024.
DOI: https://doi.org/10.1109/MNET.2023.3337141

[3] P. Blount, "Satellites are just things on the internet of things," *Air and Space Law*, Vol. 42, No. 3, pp. 273-293, May 2017.
DOI: https://doi.org/10.54648/aila2017019

[4] H. Caudill, "Big risks in small satellites: The need for secure infrastructure as a service," in *Proc. AIAA Scitech 2020 Forum*, pp. 1-10, Orlando, FL, USA, Jan. 2020.
DOI: https://doi.org/10.2514/6.2020-4017

[5] I. Altaf, M. A. Saleem, K. Mahmood, S. Kumari, P. Chaudhary, and C. M. Chen, "A lightweight key agreement and authentication scheme for satellite-communication systems," *IEEE Access*, Vol. 8, pp. 12045-12054, Mar. 2020.
DOI: https://doi.org/10.1109/ACCESS.2020.2978314

[6] J. Pavur, D. Moser, V. Lenders, and I. Martinovic, "Secrets in the sky: On privacy and infrastructure security in DVB-S satellite broadband," in *Proc. ACM SIGSAC Conf. Comput. Commun. Secur.*, pp. 230-241, London, U.K., May.1, 2019.
DOI: https://doi.org/10.1145/3317549.3323418

[7] M. Kang, S. Park, and Y. Lee, "A survey on satellite communication system security," *Sensors*, Vol. 24, No. 9, p. 2897, May 2024.
DOI: https://doi.org/10.3390/s24092897

[8] M. Önen and R. Molva, "Denial of service prevention in satellite networks," in *Proc. IEEE Int. Conf. Commun. (ICC)*, pp. 3649-3653, Paris, France, Jun.20~24, 2004.
DOI: https://doi.org/10.1109/ICC.2004.1313376

[9] X. Su, G. Zhang, and J. Liu, "Security challenges and approaches in satellite communication systems," *IEEE Trans. Aerosp. Electron. Syst.*, Vol. 56, No. 8, pp. 780-792, Apr. 2020.
DOI: https://doi.org/10.1109/TAES.2019.2953509

[10] J. Pavur and I. Martinovic, "Exploiting DVB-S protocol vulnerabilities in small satellite networks," in *Proc. 2020 USENIX Secur. Symp.*, Boston, MA, USA, Aug. 2020, pp. 1310-1320.
DOI: Currently unavailable.

[11] A. Belapurkar, G. R. Gangadharan, and A. Simha, "Satellite cybersecurity: Threats and mitigation strategies," *IEEE Commun. Mag.*, Vol. 56, No. 10, pp. 40-46, Oct. 2018.
DOI: https://doi.org/10.1109/MCOM.2018.1800146

[12] Y. Wang, P. Liu, and Z. Chen, "Quantum encryption for secure satellite communications in the new space era," *J. Cryptogr. Eng.*, Vol. 12, No. 2, pp. 159-172, Apr. 2021.
DOI: https://doi.org/10.1007/s13389-020-00231-7

[13] M. Kübler and J. Wilson, "Analyzing signal jamming and spoofing in low Earth orbit satellites," *Int. J. Satell. Commun.*, Vol. 39, No. 5, pp. 651-663, Sep. 2021.
DOI: https://doi.org/10.1002/sat.1397

[14] Y. Deng and W. Luo, "Post-quantum cryptography for small satellite networks: A practical approach," *IEEE Trans. Aerosp. Electron. Syst.*, Vol. 55, No. 12, pp. 915-924, Dec. 2019.
DOI: https://doi.org/10.1109/TAES.2019.2953509

[15] G. Curzi, D. Modenini, and P. Tortora, "Large Constellations of Small Satellites: A Survey of Near Future Challenges and Missions," *Aerospace*, Vol. 7, No. 9, p. 133, 2020.
DOI: https://doi.org/10.3390/aerospace7090133

[16] Ashraf, I., Narra, M., Umer, M., Majeed, R., Sadiq, S., Javaid, F., & Rasool, N., "A Deep Learning-Based Smart Framework for Cyber-Physical and Satellite System Security Threats Detection," *Electronics*, Vol. 11, No. 4, p. 667, 2022.
DOI: https://doi.org/10.3390/electronics11040667

[17] Ali, A., and Ditta, A., "Securing Satellite Constellations: Challenges and Solutions for Next-Generation Space-Based Networks," *EasyChair Preprint*, no. 11831, Jan. 2024.
DOI: https://easychair.org/publications/preprint/l6cs

[18] He, C., Y. Zhang, J. Ke, M. Yao, and C. Chen, "Digital Twin Technology-Based Networking Solution in Low Earth Orbit Satellite Constellations," *Electronics*, Vol. 13, No. 7, p. 1260, 2024.
DOI: https://doi.org/10.3390/electronics13071260

[19] Challa, O., Bhat, G., & Mcnair, J., "CubeSec and GndSec: A Lightweight Security Solution for CubeSat Communications," in *Proc. Small Satellite Conference*, Logan, UT, USA, Aug. 2012.
DOI: https://digitalcommons.usu.edu/smallsat/2012/all2012/25/

[20] J. Li and Z. Ma, "Cyber threats in IoT-enabled small satellite systems: A survey," *IEEE Access*, Vol. 9, pp. 21345-21357, Feb. 2021.
DOI: https://doi.org/10.1109/ACCESS.2021.3054826