

MACHINE LEARNING

Secure Satellite Communications Using Machine Learning

Ankur Pal, Brijendra Gupta

Department of Information Technology, Siddhant College of Engineering, Sudumbare, Maval, Pune, Maharashtra, India

Published October 2026

Abstract

Satellite communication is an important technology for providing communication services over large geographical areas and for transmitting sensitive military, navigational, commercial, and other critical data. With the growth of 6G, IoT, and Low Earth Orbit (LEO) satellite constellations, secure satellite communication has become increasingly important. However, wireless and broadcast characteristics expose satellite networks to eavesdropping, spoofing, jamming, signal interference, and intrusion attacks. This paper presents an AI-driven security framework based on Machine Learning (ML), Deep Learning, Reinforcement Learning (RL), and Federated Learning. One-Class SVM and Sparse Autoencoder are considered for physical-layer authentication; LSTM/RNN models are used for telemetry anomaly and intrusion detection; CNN/CNN-LSTM models are used for jamming detection; RL is used for adaptive beamforming and artificial-noise power allocation; and Federated Learning supports privacy-preserving collaborative training. The proposed architecture integrates these modules to provide adaptive satellite-security capabilities. The stated performance values are project targets and require experimental validation.

Keywords: Satellite security; Machine Learning; Deep Learning; LEO; jamming detection; intrusion detection; physical-layer authentication; reinforcement learning; federated learning

1 Introduction

Satellite communication is an important technology for providing communication services over large geographical areas. It supports the transmission of sensitive military, navigational, commercial, and other critical data. With the growth of 6G, IoT, and Low Earth Orbit (LEO) satellite constellations, the importance of secure satellite communication is increasing [1].

Satellite communication networks are vulnerable to several security threats because of their wireless and broadcast nature. Major threats include eavesdropping, spoofing, jamming, signal interference, and intrusion attacks. LEO satellite systems also experience Doppler shifts and rapidly changing communication conditions, making security mechanisms based only on fixed thresholds difficult to maintain [2].

Traditional cryptographic security mechanisms provide an important foundation for protecting satellite communication, but they are generally designed around predefined security mechanisms. Machine Learning can complement these approaches by analyzing communication and physical-layer characteristics to identify abnormal or malicious behavior. ML techniques can be applied to RF fingerprinting, Doppler-shift analysis, received-power analysis, intrusion detection, and jamming detection [2, 3].

Deep Learning techniques such as CNN and LSTM can be used for interference and anomaly detection, while Reinforcement Learning can support adaptive beamforming and artificial-noise power allocation for secure transmission. Federated Learning can enable multiple ground stations to train models without directly sharing their raw data, supporting privacy-preserving security [1, 3, 4].

2 Security threats and machine learning techniques

Satellite communication systems, particularly LEO satellite networks, are exposed to several security threats because communication takes place through wireless channels and over long propagation distances [1].

2.1 Major security threats

Eavesdropping: An unauthorized party may intercept satellite communication signals and attempt to obtain sensitive information. The broadcast nature of satellite communication increases the importance of protecting transmitted data [1].

Spoofing: An attacker attempts to transmit a false or unauthorized signal that appears to be a legitimate satellite or communication source. Machine-learning-based physical-layer authentication can help identify abnormal signal characteristics [2].

Jamming: Jamming intentionally introduces interference into a communication channel to reduce or prevent successful communication. Deep learning can be applied to frequency-domain or spectrogram information for jamming detection [1, 4].

Intrusion Attacks: Attackers may attempt to access or manipulate satellite-network resources and telemetry. An Intrusion Detection System can analyze network or telemetry behavior and identify anomalous activities [1, 3].

Doppler and Signal Variation: LEO satellites experience significant Doppler variation because of their movement relative to ground stations. Doppler shift and received power can therefore be used as features for machine-learning-based authentication [2].

2.2 Machine learning techniques for satellite security

Table 1. Machine learning techniques for satellite security.

Security Requirement	ML Technique	Purpose
Physical-layer authentication	One-Class SVM, Autoencoder	Identify legitimate and anomalous signals
RF fingerprinting	Machine Learning	Identify signal characteristics
Intrusion detection	LSTM, RNN	Detect abnormal telemetry/network behavior
Jamming detection	CNN, Deep Learning	Identify interfering signals
Secure transmission	Reinforcement Learning	Optimize beamforming and power allocation
Privacy-preserving training	Federated Learning	Train models without sharing raw data

2.3 Role of machine learning

Table 1 summarises the machine learning techniques for satellite security. The proposed system uses One-Class SVM (OCC-SVM) and Sparse Autoencoder for physical-layer authentication. Features such

as Doppler Shift, Received Power, Carrier Frequency Offset, and IQ imbalance can be analyzed to distinguish legitimate satellite signals from anomalous or spoofed signals [1, 2].

For intrusion and jamming detection, the proposed methodology uses CNN-LSTM and LSTM-based models. Spectrum information can be converted into spectrogram images and analyzed using CNN-based models to identify interfering carriers, while LSTM models can detect anomalies in satellite telemetry [1, 3, 4].

3 ML-based intrusion detection, authentication and anti-jamming

3.1 ML-based intrusion detection

An Intrusion Detection System monitors satellite communication and telemetry data to identify abnormal or potentially malicious activities. The proposed system uses LSTM and RNN-based models for telemetry anomaly detection. LSTM is useful for analyzing sequential data because satellite telemetry and network activities can change over time. The system can classify observed behavior as normal or anomalous and generate a threat indication [1].

3.2 Physical layer authentication

Physical Layer Authentication verifies whether a received satellite signal originates from a legitimate communication source. The proposed system extracts Doppler Shift, Received Power, Carrier Frequency Offset, and IQ imbalance/RF fingerprint. These features are provided to One-Class SVM and Sparse Autoencoder models. A legitimate satellite signal is expected to have a characteristic feature distribution, while a spoofed signal may appear as an anomaly [1, 2].

3.3 ML-based anti-jamming

Jamming is an intentional interference technique that can disrupt satellite communication. The proposed methodology converts spectrum information into spectrogram images and uses CNN-based deep learning to detect interfering carriers. A CNN-LSTM approach is also proposed for detecting interfering carriers, while LSTM is used for telemetry anomaly detection [1].

3.4 Integrated security framework

The three modules can operate together as an integrated security system: Satellite signal → feature extraction → authentication → intrusion detection → jamming detection → security response.

The authentication module examines physical-layer characteristics. The IDS monitors communication and telemetry behavior, while the anti-jamming module analyzes the spectrum for interference. The combination addresses different threats rather than depending on a single security mechanism.

4 Proposed AI-driven secure satellite communication system

4.1 System architecture

The proposed communication flow is: Ground User → ML Encryption & Key Generation → Uplink with Artificial Noise → LEO Satellite → On-board Trust Management & IDS → Downlink → Ground Station → RF Authentication & Anomaly Detection → Decryption. The models selected for each module are listed in Table 2.

4.2 Major components

ML Encryption and Key Generation Module: The ground user initiates secure communication through an ML-supported encryption and key-generation module. The uplink can additionally contain artificial noise to improve communication security.

Physical Layer Authentication Module: The receiving system extracts Doppler Shift, Received Power, Carrier Frequency Offset, and IQ imbalance/RF fingerprint. OCC-SVM and Sparse Autoencoder are used to identify legitimate signals and detect anomalous or spoofed signals.

Intrusion Detection Module: An IDS continuously analyzes satellite telemetry and communication behavior. The proposed system uses LSTM-based anomaly detection and related deep-learning approaches.

Anti-Jamming Module: The spectrum is converted into spectrogram images, which are analyzed using CNN/CNN-LSTM models to identify interfering carriers and jamming activity.

Reinforcement Learning-Based Adaptive Security: An RL agent such as DQN or PPO receives information such as channel-state information and eavesdropper location and determines suitable beamforming and artificial-noise power.

Federated Learning Module: Multiple ground stations train their local security models and share model weights rather than raw data with a central aggregator, providing privacy-preserving collaborative training.

4.3 Proposed ML model selection

Table 2. Proposed ML model selection.

Module	Proposed Technique	Main Function
Authentication	OCC-SVM, Sparse Autoencoder	Detect abnormal/spoofed signals
Jamming Detection	CNN, Deep Learning Carrier Detector	Detect interfering carriers
Intrusion Detection	LSTM, RNN	Telemetry anomaly detection
Adaptive Security	DQN / PPO	Adaptive beamforming and power allocation
Privacy-Preserving Training	Federated Learning	Distributed privacy-preserving training

4.4 Working of the proposed system

1. The ground user generates and encrypts the communication data.
2. The encrypted information is transmitted toward the LEO satellite with artificial noise.
3. The satellite monitors the communication using its onboard IDS and trust-management module.
4. The received signal is analyzed for physical-layer characteristics.
5. The authentication module detects legitimate or anomalous signals.
6. The anti-jamming module analyzes the spectrum for interfering carriers.
7. The IDS analyzes telemetry for abnormal behavior.
8. The reinforcement-learning agent can adapt beamforming and artificial-noise power according to the communication environment.

9. Ground stations participate in federated training without directly sharing raw data.
10. The authenticated information is finally passed for decryption at the ground station.

5 Results and performance analysis

The proposed system is designed to provide security against spoofing, jamming, intrusion, and unauthorized access. Detection accuracy, secrecy rate and latency are identified, as the major evaluation parameters; the full set of performance parameters is listed in Table 3.

- Jamming and spoofing detection: target of 95%+ detection accuracy.
- Improved secrecy rate: expected improvement of approximately 30–40% compared with fixed power allocation.
- Low-latency authentication: target latency of less than 50 ms.
- Real-time security monitoring: proposed dashboard showing threat score, satellite trust value, and secure-link status.

5.1 Performance parameters

Table 3. Performance parameters.

Performance Parameter	Purpose
Detection Accuracy	Measures the ability to correctly detect attacks
Precision	Measures how many detected attacks are actually attacks
Recall	Measures how many actual attacks are successfully detected
F1-Score	Provides a combined measure of precision and recall
False Positive Rate	Measures incorrect classification of normal communication as an attack
Authentication Latency	Measures time required to authenticate a satellite signal
Secrecy Rate	Measures secure communication performance
Jamming Detection Rate	Measures effectiveness of detecting interference
Computational Cost	Measures resources required to execute ML models

5.2 Performance comparison

The proposed system can be compared with conventional security mechanisms using fixed thresholds and static power allocation versus ML authentication, ML-based IDS, CNN anti-jamming, and RL-based adaptive security. Comparison can be performed using attack-detection accuracy, authentication latency, secrecy rate, and communication reliability.

6 Future scope

- Quantum Key Distribution (QKD): Integration of QKD can be investigated for future quantum-resistant satellite communication.
- Quantum AI: Quantum-enhanced AI techniques can be explored for advanced satellite-security applications.
- Onboard AI: ML models can be deployed directly on satellites using onboard AI accelerators.

- 6G Non-Terrestrial Networks: The security framework can be extended to 6G NTN architectures.
- Real-Time RF Security: SDR platforms such as HackRF or USRP can be used for real-time RF signal capture and security testing.
- Autonomous Satellite Security: Future systems could use AI to automatically detect threats and adapt communication parameters.
- Privacy-Preserving Collaborative Learning: Federated Learning can be further developed for cooperation among multiple satellite and ground-station networks.

7 Conclusion

This paper presents an AI-driven framework for secure satellite communications using Machine Learning, Deep Learning, Reinforcement Learning, and Federated Learning. The framework combines physical-layer authentication, intrusion detection, anti-jamming, adaptive security, and privacy-preserving collaborative training. One-Class SVM and Sparse Autoencoder support authentication, LSTM/RNN support telemetry anomaly detection, CNN/CNN-LSTM support jamming detection, and RL supports adaptive beamforming and artificial-noise power allocation. The proposed architecture provides a foundation for adaptive security in next-generation LEO and 6G non-terrestrial networks. The performance values in this paper should be treated as targets until implementation and experimental validation are completed.

References

- [1] Zhou F, Zhu X. Reinforcement Learning for Secure Semantic LEO Satellite Networks: Joint Fidelity-Secrecy Power Allocation. *Sensors*. 2026;26(8):2546.
- [2] Abdrabou M, Gulliver TA. *Physical Layer Authentication for Satellite Communication Systems using Machine Learning*. IEEE Open Journal of the Communications Society. 2022.
- [3] Li K, Zhou H, Tu Z, Wang W, Zhang H. *Distributed Network Intrusion Detection System in Satellite-Terrestrial Integrated Networks Using Federated Learning*. IEEE Access. 2020.
- [4] Zhu C, et al. *Jamming Recognition Based on Feature Fusion and Convolutional Neural Network*. Journal of Beijing Institute of Technology. 2022.
- [5] AI-driven secure satellite communication system using machine learning for intrusion detection, anti-jamming and adaptive authentication [project synopsis]. Unpublished.