BİNGÖL UNIVERSITY

Turkish Journal of Nature and Science

e-ISSN: 2149-6366
www.dergipark.gov.tr/tdfd

Research Article

Volume 15, Issue 3, Page 258-268, 2026

Received: 15.07.2026
Accepted: 15.09.2026
Published: 30.09.2026

DOI: https://doi.org/10.46810/tdfd.1995088

SAGSU-U-6G: A Real-Time Dynamic CNN+BiLSTM Framework for Physical-Layer Intrusion Detection in Multi-Domain 6G Networks

Onur POLAT[1], Esra SÖĞÜT[2*], Zahra Şeyh NEBİ[1]

[1] Bingöl University, Engineering and Architecture Faculty, Computer Engineering Department, Bingöl, Türkiye
[2] Gazi University, Technology Faculty, Computer Engineering Department, Ankara, Türkiye

**Corresponding author: esrasogut@gazi.edu.tr*

Abstract

The sixth-generation (6G) wireless networks introduce a fundamentally new communication paradigm by integrating heterogeneous Space–Air–Ground–User–Sea Surface–Underwater (SAGSU-U) domains into a unified architecture. Although this integration significantly enhances network connectivity and coverage, it also expands the cyberattack surface, creating new security challenges for physical-layer intrusion detection. This paper presents SAGSU-U-6G, a unified physical-layer intrusion detection framework based on a hybrid convolutional neural network and bidirectional long short-term memory (CNN+BiLSTM) architecture for real-time classification of eleven cyberattack categories plus benign traffic across six network domains. A custom Python-based dynamic physical-layer simulation environment incorporating realistic propagation models and Dwell Time mechanics was developed to generate continuous sequential data using eight physical-layer and communication-quality metrics: RSSI, SINR, Doppler, CSI, BER, jitter, PDR, and throughput. The trained model was evaluated on a continuous, chronologically ordered live streaming session of 4,371 observations, temporally isolated from the training data by a strict purge gap. Experimental results demonstrate distinct attack-dependent degradation patterns across heterogeneous communication domains and confirm that the dataset follows a realistic, heterogeneous, and highly imbalanced class distribution strictly dominated by benign traffic. The proposed model achieved an 89.64% real-time streaming classification accuracy with an average inference latency of 53.47 ms, performing competitively against unidirectional LSTM and convolutional baselines.

Keywords

6G networks, Physical layer security, Intrusion detection, CNN+BiLSTM, Heterogeneous multi-domain networks, SAGSU-U-6G

Author(s) publishing with the journal retain(s) the copyright to their work licensed under the CC BY-NC-ND 4.0.
https://creativecommons.org/licenses/by-nc-nd/4.0/

BİNGÖL ÜNİVERSİTESİ

Türk Doğa ve Fen Dergisi

e-ISSN: 2149-6366
www.dergipark.gov.tr/tdfd

Araştırma Makalesi

Cilt 15, Sayı 3, Sayfa 258-268, 2026

Alınış: 15.07.2026
Kabul: 15.09.2026
Basım: 30.09.2026

DOI: https://doi.org/10.46810/tdfd.1995088

SAGSU-U-6G: Çok Alanlı 6G Ağlarında Fiziksel Katman Saldırı Tespiti için Gerçek Zamanlı Dinamik CNN+BiLSTM Çerçevesi

Onur POLAT[1], Esra SÖĞÜT[2*], Zahra Şeyh NEBİ[1]

[1] Bingöl Üniversitesi, Mühendislik Mimarlık Fakültesi, Bilgisayar Mühendisliği Bölümü, Bingöl, Türkiye
[2] Gazi Üniversitesi, Teknoloji Fakültesi, Bilgisayar Mühendisliği Bölümü, Ankara, Türkiye

**Sorumlu yazar: esrasogut@gazi.edu.tr*

Özet

Altıncı nesil (6G) kablosuz ağlar, Uzay–Hava–Kara–Kullanıcı–Deniz Yüzeyi–Sualtı (SAGSU-U) iletişim alanlarını tek bir bütünleşik mimari altında birleştirerek yeni bir iletişim kuramsal çerçevesi sunmaktadır. Bu bütünleşik yapı, ağ bağlantısı ve kapsama alanını önemli ölçüde artırırken, aynı zamanda siber saldırı yüzeyini genişleterek fiziksel katman saldırı tespiti açısından yeni güvenlik zorluklarını da beraberinde getirmektedir. Bu çalışmada, altı ağ alanı boyunca on bir farklı siber saldırı türü ile iyi huylu trafiğin gerçek zamanlı sınıflandırılmasını gerçekleştirmek amacıyla hibrit Evrişimsel Sinir Ağı ve Çift Yönlü Uzun Kısa Süreli Bellek mimarisine dayalı bütünleşik bir fiziksel katman saldırı tespit sistemi olan SAGSU-U-6G önerilmektedir. Önerilen yaklaşımın değerlendirilmesi amacıyla dinamik Kalış Süresi algoritmalarına sahip özel bir Python tabanlı benzetim ortamı geliştirilmiş ve RSSI, SINR, Doppler, Kanal Durum Bilgisi, Bit Hata Oranı, Gecikme Dalgalanması, Paket Teslim Oranı ve verim olmak üzere sekiz fiziksel katman ve iletişim kalitesi metriğini içeren ardışık gözlemler üretilmiştir. Eğitilen model, eğitim setinden zamansal olarak izole edilmiş, kronolojik sırayla akan 4.371 örnekten oluşan canlı bir simülasyon oturumunda değerlendirilmiştir. Deneysel sonuçlar; iletişim alanlarında farklı saldırı türlerinin birbirinden ayırt edilebilir şekilde bozulmalara neden olduğunu ve normal trafiğin baskın olduğu gerçekçi, heterojen ve oldukça dengesiz bir sınıf dağılımı elde edildiğini göstermektedir. Önerilen CNN+BiLSTM modeli, gerçek zamanlı canlı akışta %89,64 doğruluğa ve 53,47 ms ortalama çıkarım gecikmesine ulaşarak tek yönlü LSTM ve evrişimsel temel modellerle rekabetçi bir performans sergilemiştir.

Anahtar kelimeler

6G ağları,
Fiziksel katman güvenliği,
Saldırı tespit sistemi,
CNN+BiLSTM,
Heterojen çok alanlı ağlar,
SAGSU-U-6G

1. INTRODUCTION

The evolution of wireless communication toward sixth-generation (6G) networks is driven by the need for ubiquitous global coverage, ultra-high data rates exceeding 1 Tbps, and seamless integration of Space, Air, Ground, User, Sea Surface, and Underwater communication domains [1]. Unlike 5G, which primarily extends terrestrial cellular networks, 6G envisions a fully integrated Space-Air-Ground-User-Sea Surface-Underwater (SAGSU-U) architecture. In this architecture, low-Earth orbit (LEO) satellite constellations, high-altitude platform stations (HAPS), unmanned aerial vehicles (UAVs), terrestrial base stations equipped with intelligent reflecting surfaces (IRS), surface vessels, and autonomous underwater vehicles (AUVs) operate as a single unified network [2].

This architectural leap introduces security challenges of unprecedented complexity [3]. Each domain operates under distinct physical conditions - free-space propagation at LEO altitude, Doppler-intensive air-to-ground channels, multipath-rich urban environments, sea-surface radio propagation at sea level, and acoustically dominated underwater channels - each with its own vulnerability profile. The attack surface is not merely expanded; it is qualitatively transformed. An adversary may exploit the acoustic propagation delays inherent to underwater channels to mount timing-based spoofing attacks, manipulate reflected-signal paths at reconfigurable ground infrastructure, or launch cross-domain jamming that exploits the relay architecture connecting aerial to ground nodes.

Existing physical layer security (PLS) research has predominantly focused on single-domain threat models [4]. Machine learning approaches proposed for 5G anomaly detection - including support vector machines, autoencoders, and shallow neural networks - lack the temporal modeling capacity required to detect the overlapping, multi-domain, multi-attack scenarios that characterize 6G environments [5]. There is, therefore, a critical gap in the literature. Existing studies have not comprehensively addressed a unified intrusion detection framework covering all six hierarchical domains simultaneously under realistic, continuously streaming, and heavily imbalanced attack conditions.

The main contributions of this work are summarized as follows:

- We design and implement a six-domain SAGSU-U-6G network topology using a highly optimized Python simulation engine featuring physical-layer formulations such as Free-Space Path Loss (FSPL) and dynamic Shannon Capacity.
- We construct a dynamic sequence dataset employing a novel Dwell Time sequence generator that ensures attack environments and domains remain temporally stable, providing the sequential consistency required for recurrent neural networks to learn realistic patterns.
- We develop and evaluate a Convolutional Neural Networks (CNN) + Bidirectional Long Short-Term Memory (BiLSTM) - based physical-layer intrusion detection framework utilizing a single-label multi-class (eleven attacks plus Normal) architecture.
- We validate it on a strictly time-isolated, continuous live-streaming session of 4,371 observations, achieving 89.64% real-time classification accuracy at an average inference latency of 53.47 ms.

Figure 1 provides real-time monitoring and dashboard of the proposed SAGSU-U-6G framework.

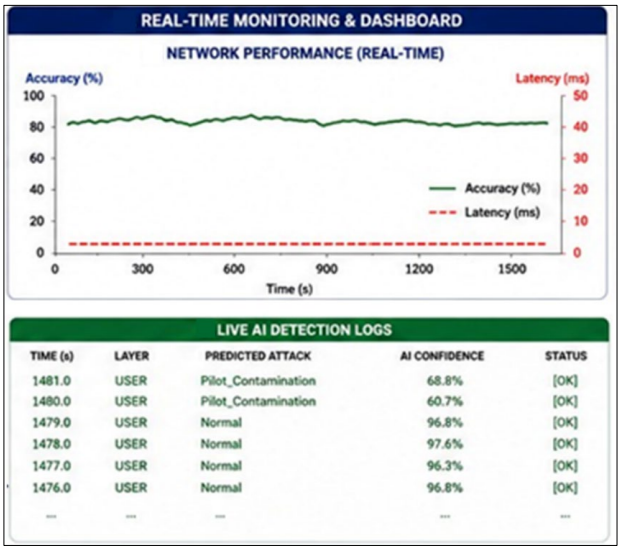


Figure 1. SAGSU-U-6G Framework Real-Time Monitoring and Dashboard

The remainder of this paper is organized as follows. Section 2 reviews related work. Section 3 describes the SAGSU-U network model and threat taxonomy. Section 4 presents the simulation methodology and dataset construction. Section 5 details the CNN+BiLSTM architecture. Section 6 reports experimental results and analysis. Section 7 discusses limitations and future directions, and Section 8 concludes the study.

2. RELATED WORK

2.1. Physical Layer Security in Heterogeneous Networks

Physical layer security leverages the inherent randomness of wireless channels - expressed through metrics such as SINR, channel capacity, and secrecy capacity - to provide information-theoretic security guarantees [6]. Early PLS work focused on single-link scenarios under passive eavesdropping models. Extensions to multi-antenna systems, notably massive MIMO, and beamforming-based secrecy, have been extensively studied for terrestrial 5G [7]. However, the multi-domain relay architectures of SAGSU-U networks introduce relay-based attacks and cross-domain interference patterns that single-domain PLS models cannot capture.

2.2. Machine Learning for Intrusion Detection in Wireless Networks

Data-driven intrusion detection systems (IDS) for wireless networks have advanced considerably with the increasing adoption of deep learning techniques. Convolutional neural networks are effective at learning local feature representations from physical-layer measurements, while recurrent neural networks, particularly LSTM-based architectures, capture temporal dependencies within sequential observations [8,9]. Hybrid deep learning architectures combining convolutional and recurrent networks have been increasingly adopted for cybersecurity and intrusion detection applications [10]. Bidirectional recurrent models further exploit both preceding and succeeding observations within a sequence, making them particularly suitable for sliding-window attack classification where attack boundaries may overlap [11]. However, existing deep learning-based IDS models have largely been developed for terrestrial wireless networks and do not explicitly consider the heterogeneous propagation characteristics and overlapping attack scenarios encountered in SAGSU-U-6G environments.

2.3. Security in Multi-Domain 6G Architectures

Recent studies have highlighted the security challenges of heterogeneous integrated networks, emphasizing the need for unified protection mechanisms across multiple communication domains. While substantial progress has been achieved for terrestrial, satellite, and UAV communications, maritime and underwater security remain comparatively less explored, particularly from the perspective of physical-layer intrusion detection. Existing studies primarily investigate individual communication segments and do not comprehensively address overlapping multi-domain attack scenarios within a unified deep learning framework [12-14].

2.4. 6G-Specific Threats

Pilot contamination remains a critical security threat in massive MIMO systems, where adversaries transmit forged pilot sequences to corrupt channel state information (CSI), resulting in degraded channel estimation and beamforming performance [15]. In parallel, cross-domain jamming and beam sniffing present novel attack vectors in integrated SAGSU-U networks, exploiting the coordination between domains and the directional nature of 6G beamforming, respectively. To the best of our knowledge, existing studies have generally investigated these threats independently and have not comprehensively evaluated them together within a unified multi-domain deep learning-based intrusion detection framework. This observation motivates their inclusion as representative 6G-specific attack scenarios in the proposed SAGSU-U-6G framework.

3. SYSTEM MODEL AND THREAT TAXONOMY

3.1. SAGSU-U Network Architecture

Inspired by the multi-layer architecture in [12], the SAGSU-U network model consists of six hierarchical domains interconnected via multi-hop relay paths. Figure 2 shows the corresponding topology. Table 1 summarizes the node types, communication technologies, and primary physical channel characteristics for each domain.

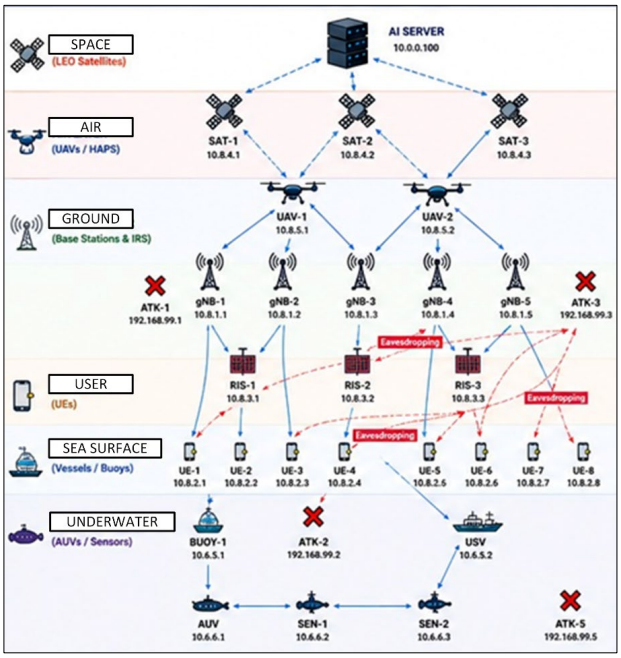


Figure 2. SAGSU-U-6G Network Topology

Table 1. SAGSU-U Network Layer Specification

Domain	Nodes	Technology	Key Channel Characteristics
Space	SAT-1, SAT-2, SAT-3, CORE	FSO / THz Inter-Satellite Links	High path loss, lower propagation delay (LEO), high Doppler shift
Air	UAV-1, UAV-2, HAPS	mmWave / Sub-THz	High Doppler, atmospheric turbulence, mobile relay channels
Ground	GNB-1 to GNB-5, IRS	Sub-6GHz / mmWave	Multipath fading, urban blockage, IRS-assisted propagation
User	UE-1 to UE-8	5G NR (FR1/FR2)	Rich scattering, pedestrian mobility, small-scale fading
Sea Surface	BUOY-1, USV	RF / Satellite uplink	Sea-surface reflection, sea-state fading, spray attenuation
Underwater	AUV, SEN-1, SEN-2	Acoustic (OFDM)	1500 m/s sound propagation, long delay spread, multipath, frequency-dependent absorption

3.2. Threat Taxonomy

We define eleven attack categories spanning conventional wireless threats, 5G-era attacks, and novel 6G-specific vectors. Table 2, based on existing security threat classifications for 6G-enabled systems [15, 16], presents the threat taxonomy adopted in this study. Table 2 extends

the classification to cover the SAGSU-U domains and associates each threat with its observable fundamental signature. Together with the benign (normal) class, these eleven categories define the twelve-class classification target used throughout this study.

Table 2. SAGSU-U-6G Threat Taxonomy

Attack Type	Class	Affected Domains	Primary Physical Signature
Jamming	DoS	All wireless domains	SINR degradation, elevated noise floor
Spoofing	Deception	Ground, User, Air	CSI inconsistency, RSSI anomaly, localization mismatch
Interception	Passive	All	No direct PHY-layer signature
Eavesdropping	Passive	All	No observable PHY metrics; inferred via higher-layer security mechanisms
Replay	Active	User, Ground	Increased latency, jitter, sequence/timestamp anomalies
Man-in-the-Middle (MITM)	Active	User, Ground, Air	CSI asymmetry, throughput degradation, delay increase
DoS	DoS	All	Throughput degradation, packet loss, increased latency
Pilot Contamination	6G-Specific	Ground (Massive MIMO)	CSI estimation error, beamforming degradation
Beam Sniffing	6G-Specific	Ground, Air, User	Beam alignment error, beam switching anomalies
Cross-Domain Jamming	6G-Specific	Multi-Domain	Correlated inter-layer interference
Underwater Spoofing	6G-Specific	Sea Underwater	Acoustic propagation delay anomaly, synchronization error

3.3. Physical Feature Vector

For each node and each time step, an eight-dimensional feature vector is extracted, encompassing eight physical-layer and communication-quality metrics: x = [RSSI, SINR, Doppler, channel state information (CSI), bit error rate (BER), Jitter, package delivery rate (PDR), Throughput]. These physical-layer and communication-quality metrics were selected based on their established relationship with wireless attack behavior and their observability within the proposed monitoring framework (Figure 1). In our custom physical simulation engine, active attacks directly manipulate these features through mathematical channel models. For instance, jamming attacks are mathematically modeled to reduce SINR logarithmically while artificially increasing the RSSI noise floor. Conversely, attacks like Pilot Contamination and IRS Manipulation directly decay the Frobenius norm of the CSI matrix. BER, PDR, and throughput quantify communication quality degradation caused by denial-of-service and active forwarding attacks. Doppler inconsistencies, when jointly analyzed with CSI or localization information, may indicate mobility- or location-spoofing attempts. Finally, abnormal jitter and delay asymmetry are characteristic indicators of replay and MITM attacks. Passive attacks such as eavesdropping generally do not generate observable physical-layer anomalies in the simulation space, deliberately challenging the deep learning model's predictive capabilities, and therefore require higher-layer security mechanisms for reliable detection.

4. PYTHON-BASED SIMULATION METHODOLOGY AND DATASET CONSTRUCTION

4.1. Simulation Environment

Unlike traditional network simulators, all experiments were conducted using a custom Python-based mathematical simulation engine. Domain-specific propagation models were adopted to represent heterogeneous communication environments. For instance, underwater characteristics explicitly calculate acoustic propagation delays using the speed of sound (1500 m/s), directly manipulating the Doppler and Jitter metrics to emulate realistic underwater spoofing scenarios. The simulation incorporates path loss, fading, interference, and node mobility to generate realistic physical-layer conditions for constructing the SAGSU-U-6G cyberattack dataset.

4.2. Attack Injection Engine

The attack injection engine operates on a defined Dwell Time logic (domain bounds: 40-90 steps, Attack bounds: 15-40 steps) to prevent hyper-randomization and maintain sequential integrity. Each data point is strictly assigned a single primary condition, modeled through a normal-biased weighted selector to preserve real-world traffic dominance. During execution, the engine dynamically modifies the corresponding network parameters to emulate different cyberattacks, including interference injection for jamming and identity replacement for spoofing.

4.3. Dataset Statistics

A comprehensive live streaming session consisting of 4,371 continuous, chronologically ordered observations was generated to rigorously evaluate the real-time capabilities of the model.

Table 3. Live-Session Class Distribution (N = 4,371)

Attack Type	Sample Count	Percentage (%)
Normal (Benign)	3,577	81.83
Spoofing	191	4.37
Eavesdropping	97	2.22

Table 3 Cont. Live-Session Class Distribution (N = 4,371)

DoS	90	2.06
Underwater Spoofing	87	1.99
Replay	70	1.60
Beam Sniffing	61	1.40
MITM	59	1.35
Pilot Contamination	59	1.35
Jamming	39	0.89
Cross-Domain Jamming	24	0.55
Interception	17	0.39
Total	4,371	100.0

As detailed in Table 3 and visually depicted in Figure 3, the dataset exhibits a realistic, heterogeneous, and highly imbalanced class distribution strictly dominated by benign (normal) traffic (81.83%). This effectively replicating real-world SAGSU-U network conditions in which attack events are comparatively rare and short-lived relative to ordinary operation.

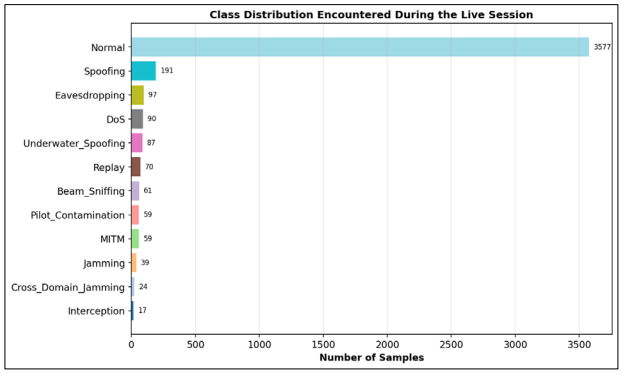


Figure 3. Class Distribution Encountered During the Live Session

4.4. Attack Impact Analysis

Attack events produce distinct changes in the observed measurements, with jamming causing the largest SINR degradation (exceeding 20 dB) and a noticeable RSSI reduction. Furthermore, heterogeneous propagation environments lead to different degradation characteristics across the six SAGSU-U domains. Representative average values measured under benign and attack conditions during the simulation calibration phase are summarized in Table 4.

Table 4. Representative Physical-Metric Degradation Under Attack Conditions

Domain	Metric	Normal Value	Attack Value	Delta
Space	SINR (dB)	25.02	17.62	−7.40 dB
Space	RSSI (dBm)	−106.72	−104.41	+2.30 dBm
User	BER	0.0000	0.0379	+0.0379
Ground	CSI (norm.)	0.949	0.868	−0.080
Sea Surface	RSSI (dBm)	-45.79	-45.79	0.00 dBm (Passive)
Underwater	Jitter (ms)	2.95	98.59	+95.63 ms

5. PROPOSED CNN+BILSTM ARCHITECTURE

5.1. Design Rationale

The classification of physical-layer attacks in SAGSU-U networks requires both effective local feature extraction and temporal sequence modeling. CNNs have demonstrated remarkable capability in automatically extracting discriminative local features through hierarchical convolutional operations, making them highly effective for learning spatial correlations among physical-layer and communication-quality metrics [17]. BiLSTM networks extend conventional LSTM architectures by processing sequential data in both forward and backward directions, thereby capturing contextual dependencies from both past and future observations [18]. The proposed CNN+BiLSTM architecture integrates these complementary strengths into a unified end-to-end framework, where CNN layers first extract representative local features and BiLSTM layers subsequently model their temporal evolution across attack sequences [19].

The BiLSTM component further exploits both preceding and succeeding observations within each attack sequence. Since multiple attacks may overlap in time, composite metric patterns (e.g. simultaneous SINR degradation caused by jamming and jitter increase caused by replay attacks) are more effectively represented using bidirectional temporal modeling than with a unidirectional recurrent network.

5.2. Architecture Specification

The proposed CNN+BiLSTM model processes input sequences of length 30, where each time step contains measurements from 8 physical-layer features collected across 6 network domains. To align the classification target with real-time causality, the labels are extracted specifically from the end of the sliding window. Temporal convolution is first applied to extract local feature representations, followed by BiLSTM layers to capture bidirectional temporal dependencies.

The final Dense output layer consists of 12 units (11 attack classes + Normal), applying Softmax activation optimized via categorical cross-entropy loss. To ensure a fair, reproducible comparison against baseline models, all evaluated architectures were constrained to representative real-world hyperparameter bounds. The Support Vector Machine (SVM) baseline used a linear kernel with C = 0.1; the Random Forest (RF) was constrained to n_estimators = 50 and max_depth = 7; the 1D-CNN baseline used two convolutional blocks with 64 and 128 filters, respectively; and the unidirectional LSTM baseline was limited to 64 recurrent units.

These constraints were applied so that inference-latency comparisons in Section 6.1 reflect models of comparable representational capacity rather than an unconstrained hyperparameter search.

5.3. Data Preprocessing and Training Protocol

The raw dataset was segmented into overlapping sequences using a sliding window of T = 30 with stride = 1. To prevent data leakage across sliding windows, sequence extraction preserves strict chronological order, splitting the data sequentially into 80% training and 20% testing. In addition, Time-Series Cross-Validation was

integrated into the training protocol to reduce variance and validate stability on the imbalanced minority classes. This approach addresses the risk that a single chronological split may produce unstable per-class metrics for attack types represented by only a few dozen samples.

A critical methodological safeguard was introduced to guarantee absolute temporal isolation between training and evaluation: a temporal gap ('purge') equal to the sliding-window size (T = 30) was inserted between the end of the training set and the beginning of the held-out live-simulation set. Since sliding windows of length T may cross the train/test boundary and introduce future information into the training data, this purge prevents any evaluation window from sharing raw observations with the training windows. The Standard Scaler normalization parameters and Label Encoder class mappings were computed exclusively on the training subset and subsequently applied, without refitting, to the held-out test data. The network was optimized using the Adam Optimizer with an Early Stopping mechanism monitoring validation loss.

The final evaluation of the trained CNN+BiLSTM model was conducted using an independent live-simulation session containing 4,371 chronologically ordered observations. This session was completely separate from the training and validation folds used during model selection. Throughout this paper, performance under this evaluation protocol is referred to as "real-time streaming accuracy". The model processes the observations as a single, continuous, time-ordered stream, thereby emulating real-world deployment conditions. Unlike a shuffled static hold-out set, this protocol preserves the temporal structure of the data during evaluation.

6. EXPERIMENTAL RESULTS AND ANALYSIS

6.1. Classification Performance

Table 5 summarizes the classification performance of the evaluated models. All baseline models (SVM, RF, 1D-CNN, and unidirectional LSTM) were evaluated under the hyperparameter constraints specified in Section 5.2. The proposed CNN+BiLSTM model was evaluated separately on the challenging, strictly continuous live-simulation stream described in Section 5.3 (4,371 samples), which was purged of any temporal overlap with the training data and contains a highly imbalanced tail of minority attack classes.

Parameters such as accuracy, f1-score, precision, recall, and latency are used for performance evaluation and comparison [20,21].

Table 5. Performance Comparison of the Evaluated Models

Model	Accuracy (%)	F1-Macro (%)	Precision (%)	Recall (%)	Latency (ms)
SVM (baseline)	72.3	68.9	70.1	69.4	8
RF	81.4	79.2	80.7	78.9	12
CNN (1D)	88.7	87.3	88.1	87.6	34
LSTM (uni.)	90.2	89.4	89.9	89.1	61
CNN + BiLSTM (ours)	89.64	61.60	61.34	62.53	~53.47

On overall accuracy, CNN+BiLSTM (89.64%) is competitive with the strongest baselines, exceeding SVM, RF, and the 1D-CNN, and trailing the unidirectional LSTM by 0.56 percentage points. This narrow gap is discussed critically in Section 7.1, since it runs counter to the initial hypothesis that bidirectional temporal modeling would provide a clear advantage over a simpler recurrent baseline. The macro-averaged Precision, Recall, and F1-score of CNN+BiLSTM (61.34%, 62.53%, and 61.60%, respectively) are, however, substantially lower than its own accuracy figure and lower than the macro scores reported for the baselines. This divergence between accuracy and macro-averaged metrics is a direct consequence of class imbalance. Normal traffic accounts for 81.83% of the live-streaming session, allowing a high overall accuracy even when several rare classes are poorly classified, whereas macro-averaged metrics weight each class equally and are therefore more sensitive to poor performance on minority attack categories. As shown in Section 6.2, three classes, namely Eavesdropping, Interception, and Underwater Spoofing, achieved 0% recall during the live session. This poor class-specific performance substantially reduced the macro-F1 score despite the relatively high overall accuracy.

6.2. Layer-Specific Detection Analysis

A comprehensive, row-normalized confusion matrix (Figure 4) and a per-class Precision/Recall/F1 chart (Figure 5) were generated directly from the live-simulation outputs. The confusion matrix shows a strong diagonal for high-impact active attacks. DoS, MITM, Replay, Spoofing, and Beam Sniffing are detected with 94–98% correct classification, indicating that these attacks exhibit sufficiently distinct physical-layer signatures for the CNN+BiLSTM model to distinguish them reliably from benign traffic and from one another.

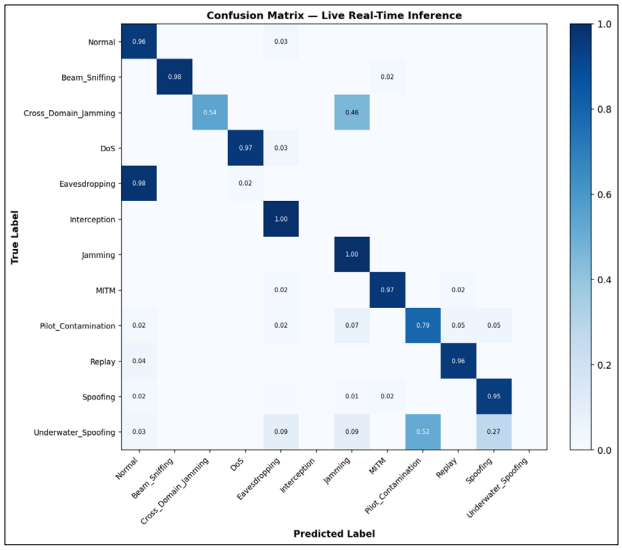


Figure 4. Confusion Matrix: Live Real-Time Inference

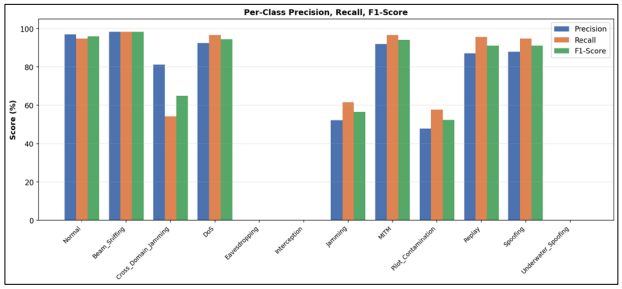


Figure 5. Per-class Precision, Recall, and F1-score

The same figures also expose the model's principal weaknesses. Eavesdropping (97 samples) and Interception (17 samples) are, by design, passive attacks with no direct physical-layer signature (Table 3). The model predicts them as Normal traffic in the overwhelming majority of cases, yielding 0% recall for both classes. Underwater Spoofing (87 samples) is correctly identified in only 27% of cases and is most frequently confused with Pilot Contamination (52% of true Underwater Spoofing instances) and, to a lesser extent, Jamming, reflecting the overlapping acoustic-domain jitter and Doppler signatures these attacks share. Cross-Domain Jamming (24 samples) is similarly split between its own class (54%) and Pilot Contamination (46%), consistent with its correlated, multi-domain interference signature bleeding into other CSI-sensitive attack types. Pilot Contamination itself achieves comparatively modest precision (47.9%) because it becomes the default 'catch-all' prediction for several of these confusable minority classes.

Table 6 and Figure 6 present the domain-wise detection accuracy, computed by attributing each live-session prediction to the network domain in which the corresponding node resides.

Table 6. Domain-Wise Detection Accuracy Values

Domain	Accuracy (%)	N
Sea Surface	94.65	1,196
User	92.33	613
Underwater	90.25	513
Space	86.31	745
Ground	85.65	481
Air	85.30	823

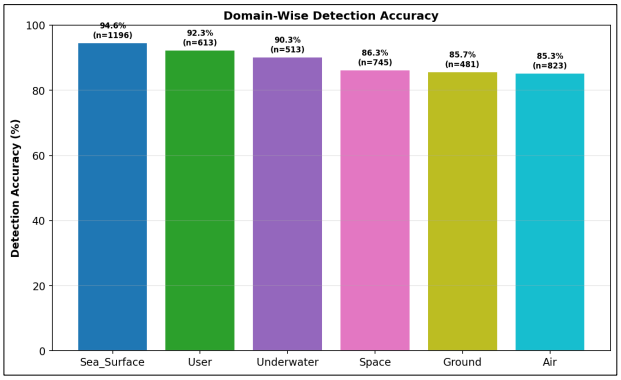


Figure 6. Domain-Wise Detection Accuracy Chart

Detection accuracy ranges from 94.65% (Sea Surface) down to 85.30% (Air), a spread of 9.35 percentage points. Sea Surface, User, and Underwater domains achieve the highest accuracy, likely because the attack types most strongly associated with these domains (Beam Sniffing, MITM, Spoofing) also happen to be among the best-recognized classes overall. Space, Ground, and Air domains show comparatively lower accuracy, consistent with their higher exposure to Cross-Domain Jamming and to passive threats that are harder to localize from physical-layer evidence alone.

6.3. 6G-Specific Attack Detection

Table 7 provides information on Per-Class Precision, Recall, and F1 Score for live sessions.

Table 7. Per-Class Precision, Recall, and F1-Score (Live Session)

Attack Type	Precision (%)	Recall (%)	F1 (%)	N
Normal	97.0	94.9	95.9	3,577
Beam Sniffing	98.4	98.4	98.4	61
Cross-Domain Jamming	81.2	54.2	65.0	24
DoS	92.6	96.7	94.6	90
Eavesdropping	0.0	0.0	0.0	97
Interception	0.0	0.0	0.0	17
Jamming	52.2	61.5	56.5	39
MITM	91.9	96.6	94.2	59
Pilot Contamination	47.9	57.6	52.3	59
Replay	87.0	95.7	91.2	70
Spoofing	87.9	94.8	91.2	191
Underwater Spoofing	0.0	0.0	0.0	87

The three 6G-specific attack types which are Beam Sniffing, Pilot Contamination, and Underwater Spoofing, present markedly different detection outcomes despite sharing a common '6G-specific' designation. Beam Sniffing achieved near-perfect recognition (98.4% precision and recall) owing to the rapid, distinctive CSI fluctuations produced by beam-alignment errors, which are well captured by the CNN feature extractor. Pilot

Contamination is detected with moderate reliability (recall 57.6%), reflecting genuine CSI-estimation-error signatures that are nonetheless confusable with the acoustic-domain classes described above. Underwater Spoofing is the weakest of the three, with a class-level recall of 0% and a normalized confusion-matrix diagonal accuracy of only 27%. This result suggests that jitter- and Doppler-based timing anomalies alone are insufficient for reliable discrimination when acoustic propagation effects overlap with other CSI-degrading conditions in the underwater domain.

6.4. Real-Time Dashboard Demonstration

A dynamic, real-time monitoring dashboard visually tracks the SAGSU-U intrusion detection framework's live operations, integrating network topology, live physical-layer measurements, detection statistics, and alert logs into a unified interface. Figure 7 presents the cumulative and rolling (window = 100 samples) accuracy of the CNN+BiLSTM model over the full 4,371-sample live session.

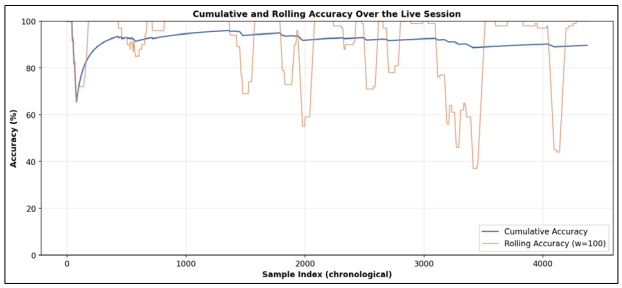


Figure 7. Cumulative and Rolling Accuracy Over the Live Session

The cumulative accuracy curve stabilizes rapidly after an initial cold-start transient (the first few hundred samples, dominated by an early cluster of minority-class attacks) and converges to the reported 89.64% by the end of the session. The rolling accuracy trace is considerably more volatile, repeatedly dipping toward 40–70% during localized bursts of hard-to-classify minority attacks before recovering. This behavior is expected given the Dwell Time attack-injection mechanism, in which attacks occur in temporally contiguous bursts rather than being uniformly interleaved. Consequently, short segments of the stream can be dominated by attack types that are difficult for the model to detect, even though its long-run cumulative accuracy remains high. During the extended live-streaming analysis window, the CNN+BiLSTM pipeline maintained an average inference latency of 53.47 ms (95th percentile: 60.44 ms). This latency is well within typical sub-100 ms real-time monitoring budgets for 6G physical-layer defense, although it is not the lowest among the models evaluated in this study, as discussed in Section 7.1.

7. DISCUSSION, LIMITATIONS AND FUTURE RESEARCH DIRECTIONS

7.1. Discussion and Limitations

The experimental results demonstrate that the proposed SAGSU-U-6G framework provides competitive physical-layer intrusion detection across heterogeneous 6G network domains. The CNN+BiLSTM model achieved an overall classification accuracy of 89.64% during the continuous live-streaming evaluation. The confusion-matrix analysis further showed strong detection performance for active and sequence-sensitive attacks, particularly MITM, Replay, DoS, and Beam Sniffing. These results suggest that the combination of convolutional feature extraction and bidirectional temporal modeling can effectively capture the physical and sequential characteristics of several active attack types.

However, the proposed CNN+BiLSTM model did not achieve the highest aggregate accuracy among the five evaluated approaches. The unidirectional LSTM baseline achieved an accuracy of 90.2%, exceeding the CNN+BiLSTM model by 0.56 percentage points. This difference should be interpreted in the context of the evaluation protocols. The CNN+BiLSTM model was evaluated on a continuous and chronologically ordered live stream containing 4,371 samples. The stream exhibited substantial class imbalance and temporally clustered rare-attack events. In contrast, the baseline results were obtained using the fixed 80/20 chronological split described in Section 5.3 without the same live-streaming purge protocol. Therefore, the evaluation conditions are not fully equivalent, and direct comparisons should be interpreted with caution.

The additional capacity of the CNN+BiLSTM architecture also does not necessarily guarantee better generalization. This is particularly relevant when the available physical-layer features contain insufficient discriminative information. Eavesdropping and Interception achieved 0% recall under the current feature formulation. Underwater Spoofing also showed limited detection performance. These attacks were intentionally modeled with absent or weakly overlapping physical-layer signatures. Consequently, their poor detection is consistent with the defined threat model rather than being solely attributable to insufficient model capacity or training.

The latency results reveal a similar trade-off. The CNN+BiLSTM pipeline achieved an average inference latency of 53.47 ms, compared with 61 ms for the unidirectional LSTM. However, the 1D-CNN baseline achieved a substantially lower latency of 34 ms while maintaining a comparable accuracy of 88.7%. The proposed model therefore provides a favorable accuracy-latency trade-off relative to the LSTM baseline, but it is not the fastest architecture evaluated. The 1D-CNN remains a strong alternative when deployment requirements prioritize inference speed and a small reduction in classification accuracy is acceptable.

The main empirical strength of the bidirectional architecture appears in its detection of sequential and boundary-sensitive active attacks. MITM, Replay, and DoS each achieved F1 scores above 91%. Access to temporal context in both directions may help distinguish transitions between benign and malicious behavior.

However, this class-specific advantage is not fully reflected in aggregate accuracy or macro-F1 scores. Future evaluations should therefore complement aggregate metrics with class-specific performance and latency analyses.

Another important limitation concerns the interpretation of the overall accuracy. The reported accuracy of 89.64% should not be interpreted as uniform protection across all eleven attack categories. In particular, the inability to reliably detect Eavesdropping and Interception represents a clear capability gap. Addressing this limitation may require information from higher network layers rather than additional physical-layer feature engineering alone.

Finally, the evaluation was conducted entirely within a Python-based physical propagation simulation. The simulation incorporates path loss, fading, Doppler effects, and acoustic propagation delays across the considered domains. Nevertheless, simulation cannot fully reproduce real-world hardware impairments, RF front-end nonlinearities, interference patterns, and rapidly changing environmental conditions. Validation on physical communication platforms is therefore required before the proposed framework can be considered suitable for practical deployment.

7.2. Future Research Directions

Future research will extend the SAGSU-U-6G framework toward more realistic, distributed, and robust security mechanisms. One direction will investigate federated learning for privacy-preserving collaborative training across heterogeneous SAGSU-U nodes. This approach could enable distributed nodes to contribute to model improvement without directly sharing raw physical-layer measurements.

The robustness of the CNN+BiLSTM architecture against adversarial perturbations will also be investigated. Such experiments will evaluate whether small and deliberately crafted modifications to physical-layer features can degrade detection performance. This analysis will provide a more comprehensive assessment of model robustness under adversarial conditions.

Complementary detection mechanisms operating above the physical layer will be explored to address the passive-attack detection gap identified in this study. This direction is particularly important for Eavesdropping and Interception, which provide insufficient discriminative evidence at the physical layer alone. Combining physical-layer observations with higher-layer behavioral or traffic information may improve the detection of these attacks.

Transformer-based attention mechanisms will also be investigated for modeling long-range temporal dependencies. Such mechanisms may be beneficial for coordinated and multi-stage attacks that evolve over longer temporal intervals. Future evaluations will additionally include class-conditional accuracy and latency analyses to provide a more detailed assessment of the trade-offs among model architectures.

Finally, hardware-assisted validation will be conducted using software-defined radio (SDR) platforms and heterogeneous communication testbeds. These experiments will assess the robustness of the proposed framework under realistic channel conditions, hardware impairments, interference, and environmental variability. Such validation will represent an important step toward evaluating the practical applicability of SAGSU-U-6G beyond simulation environments.

8. CONCLUSION

This study presented SAGSU-U-6G, a unified physical-layer intrusion detection framework for heterogeneous 6G networks spanning the Space, Air, Ground, User, Sea Surface, and Underwater domains. A Python-based physical propagation simulation was used to generate a realistic, benign-dominated, and highly imbalanced dataset covering eleven attack categories. The proposed CNN+BiLSTM architecture was evaluated under a strictly time-isolated, continuous live-streaming protocol.

The model achieved an overall classification accuracy of 89.64% with an average inference latency of 53.47 ms. Strong detection performance was observed for several active and sequence-sensitive attacks, including MITM, Replay, DoS, and Beam Sniffing. However, the model did not uniformly outperform the evaluated baselines and showed substantial limitations in detecting passive and acoustically overlapping attacks from physical-layer observations alone.

These findings demonstrate both the potential and the current limitations of deep temporal models for physical-layer intrusion detection in heterogeneous 6G environments. Rather than providing uniform protection against all attack types, SAGSU-U-6G establishes a reproducible framework for evaluating where physical-layer learning is effective and where additional security information is required. Future extensions incorporating higher-layer information, distributed learning, advanced temporal modeling, and hardware-based validation may help address the remaining detection gaps and support more robust multi-domain 6G security.

REFERENCES

[1] Giordani M, Polese M, Mezzavilla M, Rangan S, Zorzi M. Toward 6G Networks: Use Cases and Technologies. IEEE Communications Magazine. 2020;58(3):55-61.

[2] Zhang Z, Xiao Y, Ma Z, Xiao M, Ding Z, Lei X, et al. 6G Wireless Networks: Vision, Requirements, Architecture, and Key Technologies. IEEE Vehicular Technology Magazine. 2019;14(3):28-41.

[3] Tariq F, Khandaker MRA, Wong KK, Imran MA, Bennis M, Debbah M. A Speculative Study on 6G. IEEE Wireless Communications. 2020;27(4):118-125.

[4] Liu Y, Chen H-H, Wang L. Physical Layer Security for Next Generation Wireless Networks:

Theories, Technologies, and Challenges. IEEE Communications Surveys & Tutorials. 2017;19(1):347-376.
[5] Thakkar A, Lohiya K. A Review on Machine Learning and Deep Learning Perspectives of IDS for IoT: Recent Updates, Security Issues, and Challenges. Archives of Computational Methods in Engineering. 2021;28:3211-3243.
[6] Wyner AD. The Wire-Tap Channel. Bell System Technical Journal. 1975;54(8):1355-1387.
[7] Zhu J, Schober R, Bhargava VK. Secure Transmission in Multicell Massive MIMO Systems. IEEE Transactions on Wireless Communications. 2014;13(9):4766-4781.
[8] LeCun Y, Bengio Y, Hinton G. Deep Learning. Nature. 2015;521:436-444.
[9] O'Shea T, Hoydis J. An Introduction to Deep Learning for the Physical Layer. IEEE Transactions on Cognitive Communications and Networking. 2017;3(4):563-575.
[10] Xin Y, Kong L, Liu Z, Chen Y, Li Y, Zhu H, et al. Machine Learning and Deep Learning Methods for Cybersecurity. IEEE Access. 2018;6:35365-35381.
[11] Schuster M, Paliwal K K. Bidirectional Recurrent Neural Networks. IEEE Transactions on Signal Processing. 1997;45(11):2673-2681.
[12] Guo H, Li J, Liu J, Tian N, Kato N. A Survey on Space-Air-Ground-Sea Integrated Network Security in 6G. IEEE Communications Surveys & Tutorials. 2022;24(1):53-87.
[13] Cheng N, Jingchao HE, Zhisheng YIN, Conghao ZHOU, Huaqing WU, Feng LYU, et al. 6G service-oriented space-air-ground integrated network: A survey. Chinese Journal of Aeronautics. 2022;35(9):1-18.
[14] Stojanovic M, Preisig J. Underwater Acoustic Communication Channels: Propagation Models and Statistical Characterization. IEEE Communications Magazine. 2009;47(1):84-89.
[15] Marzetta TL. Noncooperative cellular wireless with unlimited numbers of base station antennas. IEEE transactions on wireless communications. 2010; 9(11): 3590-3600.
[16] Osorio DPM, Ahmad I, Sanchez JDV, Gurtov A, Scholliers J, Kutila M, et al. Towards 6G-Enabled Internet of Vehicles: Security and Privacy. IEEE Open Journal of the Communications Society. 2022;3:82-105.
[17] Alex K, Ilya S, Geoffrey EH. ImageNet Classification with Deep Convolutional Neural Networks. Communications of the ACM. 2017;60(6):84–90.
[18] Graves A, Schmidhuber J. Framewise Phoneme Classification with Bidirectional LSTM and Other Neural Network Architectures. Neural networks. 2005;18(5-6):602-610.
[19] Chiu JP, Nichols E. Named Entity Recognition with Bidirectional LSTM-CNNs. Transactions of the Association for Computational Linguistics. 2016;4:357-370.
[20] Balım C, Olgun N. Classification of Temporary and Real E-mail Addresses with Machine Learning Techniques. Turkish Journal of Nature and Science. 2024;13(3):176-183.
[21] Gündüz M Z, Daş R. An effective DNN-based Approach for Detecting Energy Theft in Smart Grids through User Consumption Patterns. Turkish Journal of Nature and Science. 2023;12(4):163-170.