ALL SCIENCES ACADEMY

5th International Conference on Modern and Advanced Research ICMAR 2026



May 07-08, 2026 | Konya, Turkey

Proceeding Book

All Sciences Academy

5th International Conference on Modern and Advanced Research

May 07-08, 2026: Konya, Turkey

© 2026 Published by All Sciences Academy

https://as-proceeding.com/index.php/icmar/home

Simulation of Physical Layer Attacks in 6G Networks Using NS-3 and Their Detection via Machine Learning

Esra Söğüt[1,*], Onur Polat[2], Zahra Şeyh Nebi[2]

[1]*Department of Computer Engineering, Faculty of Technology, Gazi University, Ankara, Türkiye*
[2]*Department of Computer Engineering, Bingöl University, Bingöl, Türkiye*

[*]*(esrasogut@gazi.edu.tr) Email of the corresponding author*

Abstract – This study addresses the simulation of attacks threatening the physical layer security of 6G wireless networks, the generation of labeled datasets, and machine learning-based attack detection. As part of this study, a multi-layer 6G topology featuring a Satellite-Air-Ground-Sea (SAGS) architecture was modeled using the NS-3 network simulator. A total of 12 attack types—including Jamming, Eavesdropping, Spoofing, DoS, Pilot Contamination, RIS Manipulation, MITM, Replay, Wormhole, Sinkhole, Blackhole, and DDoS—were simulated on this topology. A labeled dataset consisting of 33,953 samples and containing 25 features was generated from the simulations. The Random Forest, Decision Tree, and Support Vector Machine algorithms were compared on the generated dataset. According to the results, the Random Forest model demonstrated the most balanced performance with approximately 76% accuracy, 0.763 precision, 0.760 recall, and an F1 score of 0.76. The findings indicate that it is possible to model 6G-specific threats alongside classical network attacks within the same dataset and that machine learning-based approaches are applicable for real-time attack detection.

Keywords – 6G security, physical layer security, NS-3, attack detection, Random Forest, RIS manipulation, pilot contamination, SAGS

I. INTRODUCTION

Sixth-generation (6G) communication systems are expected to become widespread in the 2030s; these next-generation networks are projected to incorporate Terahertz (THz) bands, reconfigurable Intelligent Surfaces (RIS), large-scale MIMO systems, and multi-layered architectures such as Space-Air-Ground-Sea (SAGS). This architectural transformation brings to the forefront not only traditional network security issues but also new threat vectors specific to the physical layer.

In particular, attacks such as RIS manipulation and pilot contamination stand out as threats arising from 6G's structural components and having more complex effects compared to 5G. Therefore, the early detection of physical layer attacks requires moving beyond security approaches relying solely on cryptographic mechanisms [1].

The primary objective of this study is to model both classical and 6G-specific physical layer attacks within the same simulation framework in a 6G environment, generate a labeled dataset from these attacks, and evaluate the classification performance of machine learning-based methods on the dataset. The original contribution of this study lies in simulating 12 different attacks and a non-attack scenario within the same topology using NS-3, generating a dataset consisting of 33,953 samples, and comparing three different classification algorithms. The workflow diagram of the study is presented in Figure 1.

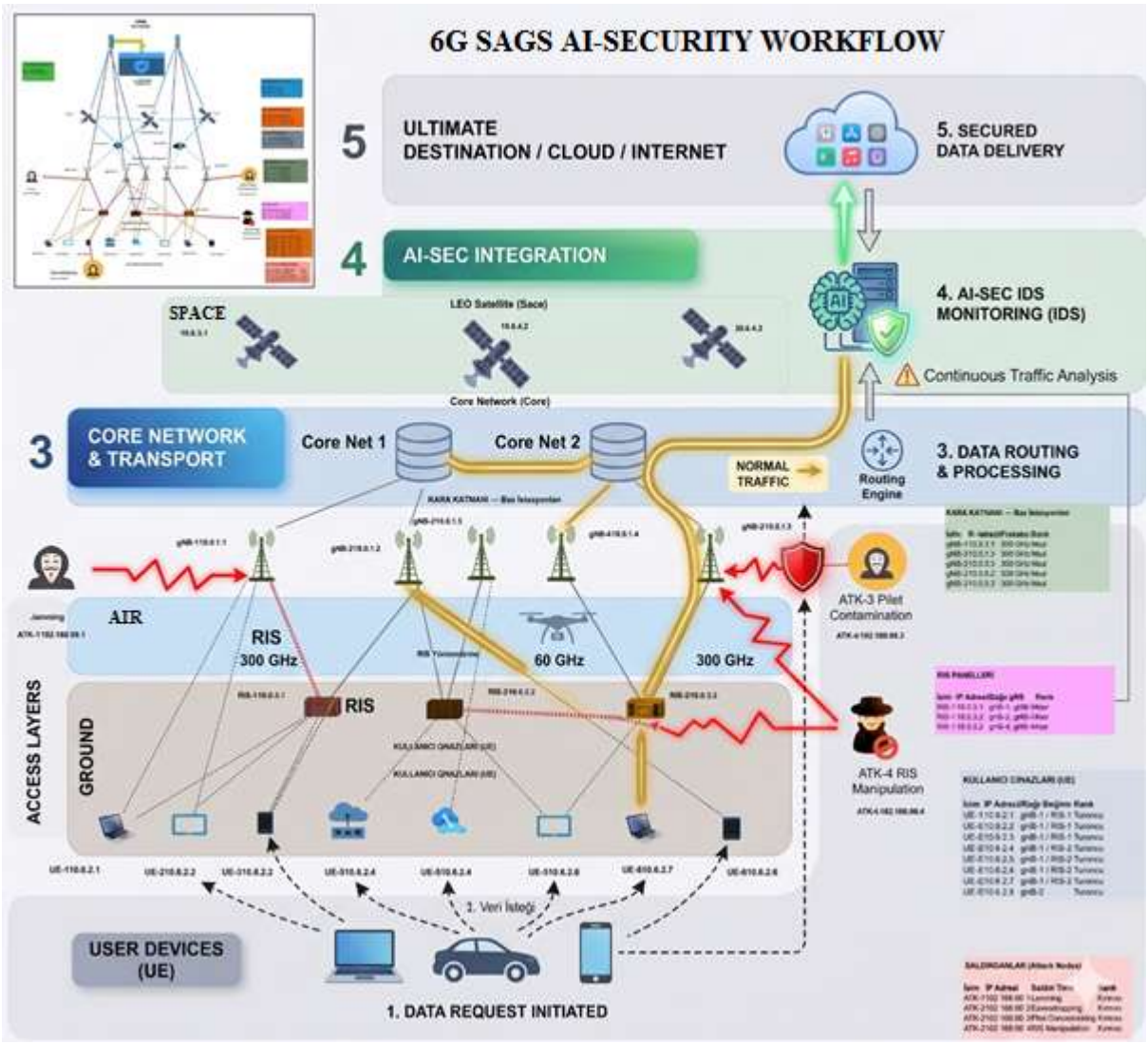


Fig. 1 6G SAGS Topology Workflow

II. Related Work

In recent years, various research directions have emerged in the field of 6G physical layer security, including deep learning, RIS optimization, XL-MIMO-based interference modeling, and NS-3-based attack detection. In the reviewed literature, attacks such as jamming, spoofing, eavesdropping, pilot contamination, and RIS manipulation have been addressed in different contexts. It is observed that there is a limited number of open-label datasets that combine multiple physical layer attacks within the same dataset.

Table 1. Summary of related studies

Study	Method / Approach	Target Attacks	Environment / Tool	Dataset
Kumar et al. [2]	RNNs, NNs, SVM (MIMO-OTFS detection)	Canal fading/interference (jamming-like)	MATLAB	Simulation-based synthetic data
Tariq et al. [3]	Beamforming for Reflective Intelligent Surfaces (RIS)	Jamming	MATLAB	Synthetic data
Lee et al.[4]	XL-MIMO interference modeling	Pilot Contamination, RIS Manipulation	MATLAB	Synthetic data
Bahety	ML-based anomaly	Anomaly (such as	NS-3 /	Synthetic data

et al. [5]	detection	jamming or spoofing)	mmWave simulation	
This study	Multi-attack detection using RF, DT, and SVM	12 attacks and normal traffic	NS-3 + Python	33,953 labeled samples

Table 1 presents a comparison of the relevant studies summarized in this work in terms of methodology, target attacks, and data set usage. Unlike the existing literature, this study models both 6G-specific attacks and classical attacks together on the same topology and provides a multi-algorithm comparison using an open data set approach.

III. Materials and Method

A. Simulation Environment

NS-3 was selected as the simulation platform for this study. NS-3 was selected because it supports physical layer modelling, is widely used in academic research, and is suitable for generating real-time CSV output [6]. Ubuntu running on WSL2 was used as the development environment. This provided the practical convenience of development on Windows while maintaining Linux compatibility.

B. SAGS-Based 6G Topology

The 6G topology consists of four main layers: space, air, ground, and user. The topology includes 3 LEO satellites, 2 UAVs, 5 6G base stations, 3 RIS panels, 2 kernel network nodes, 8 user devices, 4 attack nodes, and 1 AI-SEC server. This structure is designed according to the SAGS approach to generate different coverage areas and attack surfaces.

C. Attack Scenarios

A total of 12 attack types were modeled within the simulation: Jamming, Eavesdropping, Spoofing, DoS, Pilot Contamination, RIS Manipulation, MITM, Replay, Wormhole, Sinkhole, Blackhole, and DDoS. For each attack, separate start times, generation intervals, and distinguishing attributes were defined.

Table 2. Information on the attacks in the study

Attack	Start	Interval	C++ Function	Basic Parser Feature
Normal	0.0s	0.10s	Normal()	Reference — all values stable
Jamming	1.0s	0.03s	Jamming()	interference high, SNR low, throughput ≈ 0
Eavesdropping	2.0s	0.10s	Eavesdropping()	secrecy_rate ≈ 0, entropy_score medium
Spoofing	3.0s	0.10s	Spoofing()	auth=0, handover 8-15, frequency_offset high
DoS	4.0s	0.02s	DoS()	delay 100-600ms, pkt_loss >%60, jitter_ms high
Pilot_Contam.	5.0s	0.10s	PilotContam()	pilot_snr low, beam_mismatch high
RIS_Manip.	6.0s	0.10s	RISManip()	ris_phase 0.5-3.14 rad, beam_width wide
MITM	7.0s	0.12s	MitmAttack()	auth=0, delay medium, entropy medium
Replay	8.0s	0.15s	Replay()	delay 200-800 ms, entropy_score low
Wormhole	9.0s	0.08s	Wormhole()	doppler_shift 200-500 Hz (analytic)
Sinkhole	10.0s	0.10s	Sinkhole()	pkt_loss %80+, throughput low
Blackhole	12.0s	0.02s	Blackhole()	throughput=0, pkt_loss=%100, link_quality=0
DDoS	14.0s	0.01s	DDoS()	entropy_score=0.98, jitter 300-700 ms

Table 2 summarizes various attack models. For example, the jamming attack is modeled with high interference, low SNR, and very low throughput. The blackhole attack, on the other hand, is modeled with the signature throughput=0, pkt_loss=1, and link_quality=0.

D. Dataset Generation and Attributes

During real-time simulation, 25 attributes (15 basic + 10 new 6G-specific) were written to a CSV file for each event. Among these attributes, metrics such as snr, sinr, rssi, throughput, pkt_loss, delay, interference, ber, pilot_snr, ris_phase, beam_mismatch, channel_cap, anomaly, auth, handover are 5G-specific and basic attributes. In addition, 6G-specific metrics such as secrecy_rate, doppler_shift, beam_width, frequency_offset, channel_coherence, path_diversity, jitter_ms, retransmit_count, entropy_score ve link_quality are also included.

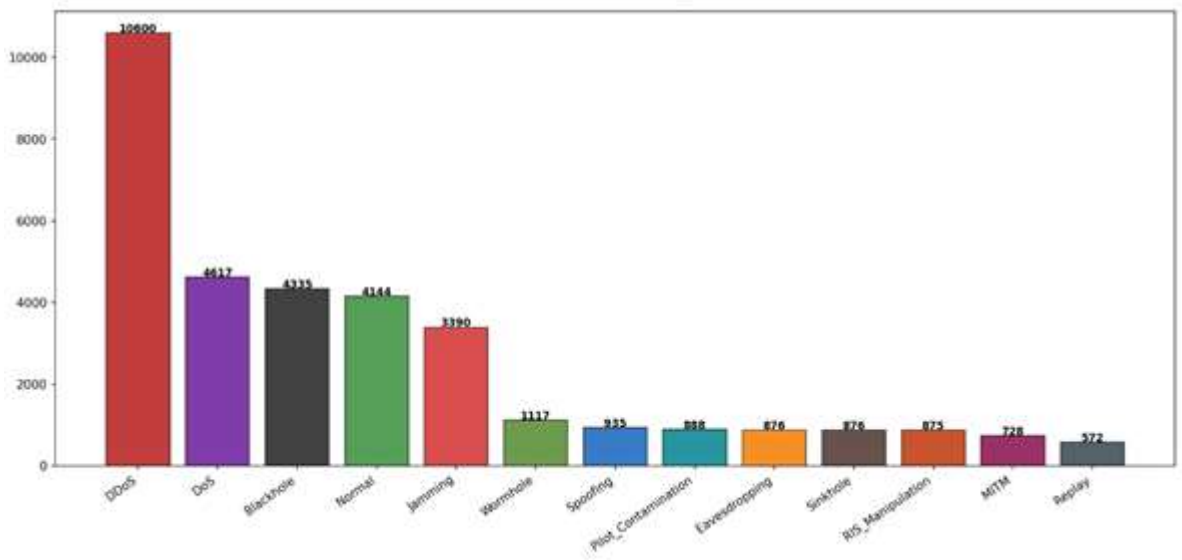


Fig. 2 Real-time simulation attack distribution (25 features, 12 attacks)

According to Figure 2, the dataset consists of a total of 33,953 samples and contains 13 classes. These classes include 12 attack types and normal traffic. In the class distribution, the highest number of samples is 10,600 for DDoS attacks, while the lowest is 572 for Replay attacks.

E. Machine Learning Models

Decision Tree, Random Forest, and Support Vector Machine algorithms were used for intrusion detection. Scaling was applied during the data pre-processing stage. The data was split into training and test sets (70% and 30%, respectively), and model stability was evaluated using 5-fold cross-validation. In the Random Forest model, 100 trees and a limited depth were used. For the SVM, the RBF kernel was chosen to capture non-linear patterns.

IV. FINDINGS

Upon analyzing the attack statistics, the average SNR value for normal traffic was recorded as 14.9 dB, and the throughput value as 1.25 Gbps. It was observed that attacks such as jamming, DoS, blackhole, and DDoS caused a significant drop in throughput. Pilot Contamination and RIS Manipulation attacks are particularly distinguished from other classes by low SNR, high beam mismatch, and ris_phase deviations.

Table 3. Summary of the distinguishing statistics of the attack classes in the study

Attack	Number of Samples	Avg. SNR	Avg. Throughput	Avg. packet loss	Avg. delay
Normal	4.144	14.9 dB	1.25 Gbps	0.01	0.34 ms
Jamming	3.390	9.9 dB	0.005 Gbps	0.797	229.3 ms

Eavesdropping	876	32.6 dB	0.79 Gbps	0.025	0.24 ms
Spoofing	935	46.4 dB	0.30 Gbps	0.321	37.1 ms
DoS	4.617	22.3 dB	0.002 Gbps	0.819	360.5 ms
Pilot_Contam.	888	-0.2 dB	0.22 Gbps	0.516	55.6 ms
RIS_Manip.	875	-10.8 dB	0.01 Gbps	0.727	94.7 ms
MITM	728	36.1 dB	0.50 Gbps	0.201	54.2 ms
Replay	572	26.7 dB	0.63 Gbps	0.144	608.2 ms
Wormhole	1.117	48.3 dB	1.00 Gbps	0.046	0.70 ms
Sinkhole	876	33.1 dB	0.12 Gbps	0.842	150.3 ms
Blackhole	4.335	30.3 dB	0.000 Gbps	1.000	1250.7 ms
DDoS	10.600	31.0 dB	0.000 Gbps	0.945	996.7 ms

According to the model comparison results, the overall accuracy rate of the three algorithms is approximately 76%. The most balanced results in terms of precision, recall, and processing time were obtained with the Random Forest model. For the Random Forest, precision was reported as 0.763, recall as 0.760, the F1 score as 0.76, and the training time as approximately 200 ms. Although the Decision Tree had a shorter training time, it exhibited a more fragile structure; the SVM, on the other hand, produced similar accuracy at a higher computational cost.

Table 4. Performance metrics of the proposed models

Model	**Accuracy**	**Precision**	**Recall**	**F1**	**Period of Training**
Random Forest	%76.0	0.763	0.760	0.76	200 ms
Decision Tree	%76.0	0.758	0.760	0.76	50 ms
SVM	%76.0	0.761	0.760	0.76	500 ms

When examining attack-based success rates, a 100% success rate was achieved in the Blackhole class, approximately 96% in the Normal class, and approximately 81% in the Wormhole class. In contrast, success rates remained very low in the MITM and Sinkhole classes, and in the Replay class, it was observed that the model could not learn sufficiently due to a lack of data.

Table 5. Success rates of attack classes

Attack Class	**Success Rate**	**Comment**
Blackhole	%100	Unique signature: throughput=0, pkt_loss=1, link_quality=0
Normal	≈%96	Reference class, maximum number of samples
Wormhole	≈%81	Doppler-based distinctive pattern
Spoofing	≈%71	Distinguished by auth and handover
Pilot Contamination	≈%76	pilot_snr and beam_mismatch are influential
DoS	≈%65	Tendency to be confused with DDoS
DDoS	≈%68	Entropy is helpful, but there is overlap with the DoS class
Eavesdropping	≈%50	Harder to detect due to passive nature
Jamming	≈%64	Partially overlaps with DoS

MITM	≈%0	Lack of unique features
Sinkhole	≈%0	Similar pattern to Blackhole
Replay	≈%4	Insufficient number of samples

V. DISCUSSION

The results of the study demonstrate that physical layer attacks in 6G networks can be more effectively distinguished not only using individual metrics but also within a multidimensional feature space. In particular, the use of variables specific to 6G, such as ris_phase, pilot_snr, doppler_shift, and entropy_score, alongside classical network security metrics has enhanced classification performance.

Conversely, the low success rates observed in certain classes highlight a significant limitation. The weak discriminative signature for MITM and Sinkhole attacks suggests that the current feature set is insufficient for these classes. Similarly, the low performance in Replay attacks is related to the small number of examples in this class.

Therefore, it is recommended that future studies incorporate new features such as MAC-layer error rate, key mismatch, route tracing, and selective drop. Additionally, more balanced data generation could be implemented for underrepresented classes. This would enable the system to learn decision boundaries more clearly, particularly between attack types that are similar to one another.

VI. CONCLUSION

In this study, 12 different physical layer and network attacks were modeled on an NS-3-based 6G SAGS topology. A labeled dataset consisting of 33,953 samples was generated, and three different machine learning algorithms were compared on this dataset. The results indicate that the Random Forest model is the most suitable candidate for real-time attack detection, achieving approximately 76% accuracy and balanced performance metrics. The primary contribution of this study is the integration of 6G-specific attacks with classical attacks within a single simulation framework, and the provision of a practical data generation and analysis pipeline for multi-class attack detection.

REFERENCES

[1] Khalid, W., Van Chien, T., Khan, W. U., Kaleem, Z., Zikria, Y. B., Kim, T., & Yu, H. (2025). Malicious reconfigurable intelligent surfaces: Security threats in 6G networks. *IEEE Internet of Things Journal,* 12:15, 30063 - 30085. 10.1109/JIOT.2025.3570544

[2] Kumar, A., Gaur, N., & Nanthaamornphong, A. (2024). Machine learning RNNs, SVM and NN algorithm for massive-MIMO-OTFS 6G waveform with Rician and Rayleigh channel. *Egyptian Informatics Journal*, 27, 100531. https://doi.org/10.1016/j.eij.2024.100531

[3] Tariq, Z. U. A., Baccour, E., Erbad, A., & Hamdi, M. (2025). RIS assisted Anti-Jamming in Next-Generation wireless communication networks: A survey of Threats, Solutions, and research challenges. *IEEE Open Journal of the Communications Society*, 6, 8714 - 8744. 10.1109/OJCOMS.2025.3621541.

[4] Lee, J. B., Kim, G. E., Kang, H., Son, H. K., & Lee, W. H. (2025). Emerging Interference Modeling and Analysis Techniques for 6G Networks: A Comprehensive Survey. *IEEE Access*, 13, 187187-187210.

[5] Bahety, P., Chopade, P., Patra, M., & Pawar, R. (2026, January). An NS-3/mmWave-Based Simulation Framework for Real-Time Anomaly Detection in UAV-Assisted 6G Networks. In the *18th International Conference on Communication Systems and Networks* (COMSNETS) (pp. 1003-1007). IEEE.

[6] Tonyalı, S. (2023). ns-3 Ağ Simülatörü ile OpenSSL Kütüphanesinin Entegre Edilmesi ve Bir Kimliği Doğrulanmış Şifrelemenin Uygulanması. *International Journal of Advanced Natural Sciences and Engineering Researches*, 7(4), 119–124. https://doi.org/10.59287/ijanser.566