Enhancing Security in 5G and Future 6G Networks: Machine Learning Approaches for Adaptive Intrusion Detection and Prevention

OGUNYEMI, A. O.[1], OLAWALE, B. O.[2], ORISAJIMI, J. O.[3], ADESIYAN A. A.[4]

[1,2,4] **Department of Computer Engineering, Faculty of Engineering, Osun State Polytechnic, Iree**.

[3]**Department of** *Electrical/Electronic Engineering, Faculty of Engineering, Osun State Polytechnic, Iree.*

Corresponding Author: ayooluwa17@gmail.com, Tel: +2347017849422

ABSTRACT

The transition from fourth-generation (4G) mobile communication systems to fifth-generation (5G) and emerging sixth-generation (6G) networks has significantly transformed wireless communications by enabling ultra-high-speed, low-latency, and highly reliable services that support a broad spectrum of applications, including the Internet of Things (IoT), smart cities, autonomous systems, and critical infrastructure. Despite these advancements, the distinctive characteristics of 5G and future 6G networks, such as massive device connectivity, heterogeneous architectures, and dynamic service orchestration, introduce substantial security challenges and expand the cyberattack surface. This paper presents a comprehensive framework for strengthening the security of current and next-generation wireless networks through the integration of advanced machine learning (ML) techniques into intrusion detection and prevention systems (IDPS). The study examines key security challenges in 5G and future 6G architectures, explores ML algorithms designed to mitigate evolving cyber threats, and discusses privacy-preserving mechanisms alongside regulatory compliance requirements under the European Union Artificial Intelligence Act. Furthermore, a Wireless Intrusion Detection Algorithm (WIDA) is proposed to enhance adaptive threat detection and automated response mechanisms. The findings demonstrate that ML-driven intrusion detection significantly improves the resilience, intelligence, and trustworthiness of wireless network security systems.

Keywords: 5G networks, 6G networks, machine learning, intrusion detection, cybersecurity, wireless network protection.

1. Introduction

The fifth generation (5G) of mobile communication networks represents a significant advancement in telecommunications, offering enhanced mobile broadband, ultra-reliable low-latency communication (URLLC), and massive machine-type communication (mMTC). These capabilities serve as the foundation for emerging applications such as the Internet of Things (IoT), smart cities, autonomous transportation systems, and remote healthcare services. (Andrews et al., 2014; 3GPP TS 33.501, 2023). However, the defining characteristics of next-generation wireless networks, including dense device connectivity, high heterogeneity, virtualization, and flexible architectures also increase their vulnerability to sophisticated cyber threats (3GPP TS 33.501, 2023).

The expansion of the attack surface and the rapidly evolving threat landscape have made traditional security mechanisms increasingly inadequate for modern wireless environments. Emerging threats such as signaling storms, distributed denial-of-service (DDoS) attacks, side-channel exploits, and adversarial manipulation of artificial intelligence models present serious challenges to network integrity and reliability. Conventional security approaches, including firewalls and static signature-based intrusion detection systems, often lack the adaptability required to effectively counter these evolving attack patterns (Sommer & Paxson, 2010). (Cisco Systems, 2023). Machine learning (ML) has emerged as a transformative approach for improving threat detection, prevention, and mitigation in current and next-generation wireless networks. ML-based intrusion detection systems can process large-scale network traffic, identify anomalous patterns associated with cyberattacks, and continuously adapt to changing traffic behavior. Studies have shown that ML-driven adaptive intrusion detection and prevention systems provide a robust security layer for complex wireless infrastructures (Bharati et al., 2021; Shafiq et al., 2020).

Supervised learning algorithms enable the classification of known attack categories with high accuracy using labeled datasets, whereas unsupervised learning techniques facilitate the detection of previously unseen threats through anomaly detection. Furthermore, deep learning architectures such as Convolutional Neural Networks (CNNs), Recurrent Neural Networks (RNNs), and Graph Neural Networks (GNNs) have demonstrated remarkable performance in extracting complex traffic patterns from large-scale network datasets (Goodfellow et al., 2016). Reinforcement learning enhances adaptive defense strategies by dynamically optimizing mitigation responses, while federated learning supports privacy-preserving collaborative intelligence across distributed wireless environments (Nguyen et al., 2022). The European Union Artificial Intelligence Act introduces a harmonized regulatory framework for artificial intelligence technologies across critical infrastructures, including telecommunications. Since wireless communication networks are classified as critical infrastructure, ML-based security systems must satisfy stringent requirements related to transparency, explainability, testing, and lifecycle management. These regulatory obligations emphasize the importance of building trustworthy, accountable, and resilient AI-driven security solutions. The novelty of this study is threefold. First, it proposes an adaptive ML-driven security framework aligned with major 6G security trends and layered wireless architecture. Second, it

introduces an optimized Wireless Intrusion Detection Algorithm (WIDA) integrated within this framework to enhance anomaly detection and automated response capabilities. Third, it bridges the gap between advanced technological innovation and emerging legal requirements by demonstrating how regulatory frameworks influence the design and deployment of ML-based security systems.

The objectives of this paper are to:

- Present a comprehensive review of machine learning approaches for adaptive intrusion detection and prevention in 5G and 6G networks.
- Analyze real-world implementations and case studies that demonstrate practical feasibility.
- Identify open challenges and future research directions for developing resilient, intelligent, and trustworthy wireless security frameworks.

2. Background on 5G and 6G Security

The security architecture of fifth-generation (5G) wireless networks builds upon the foundational principles established in fourth-generation (4G) Long-Term Evolution (LTE) systems while introducing substantial improvements in authentication, privacy, and trust management. The transition from 4G to 5G and eventually to sixth-generation (6G) networks represents a paradigm shift in network architecture, operational flexibility, and service delivery models. This evolution is driven by increasing demands for intelligent connectivity, ultra-low latency, and highly scalable communication systems (3GPP TS 33.501, 2023). The 5G security framework is generally structured into three major domains: the Access Stratum (AS), the Non-Access Stratum (NAS), and the Service-Based Architecture (SBA). Key security enhancements in 5G include the introduction of the Subscription Concealed Identifier (SUCI), which protects user identity privacy, mutual authentication through the 5G Authentication and Key Agreement (5G-AKA) protocol, and unified cryptographic key management across multiple services. These features significantly improve confidentiality, integrity, and trust within mobile communication environments. The primary 5G use cases include enhanced mobile broadband (eMBB), ultra-reliable low-latency communication (URLLC), and massive machine-type communication (mMTC). Looking ahead, 6G is expected to expand these service categories into immersive communication, massive communication, and hyper-reliable low-latency communication while incorporating emerging technologies such as AI-driven communication, integrated sensing and communication, and ubiquitous connectivity. These capabilities are expected to enable applications including digital twins, holographic communication, autonomous intelligence, and cyber-physical systems.

A defining characteristic of 5G and future 6G systems is the integration of enabling technologies such as Software-Defined Networking (SDN), Network Function Virtualization (NFV), and edge computing. These technologies support high-bandwidth communication, ultra-low latency, and dynamic network slicing for diverse vertical sectors, including industrial automation, autonomous transportation, smart healthcare, and intelligent manufacturing. Although these technologies greatly improve network efficiency and flexibility, they also introduce new attack vectors and security vulnerabilities that require adaptive and intelligent defense mechanisms.

2.1 Software-Defined Networking (SDN)

Software-Defined Networking decouples the control plane from the data plane, enabling centralized management of network resources and policies. (Kreutz et al., 2015). Unlike conventional hardware-centric networking systems, SDN abstracts network intelligence into logically centralized controllers that dynamically configure traffic flows, enforce Quality of Service (QoS) policies, and deploy security rules through programmable interfaces. This architectural flexibility enhances scalability, interoperability, and cost efficiency. Despite these advantages, SDN introduces critical security concerns. The centralized controller may become a high-value target for attackers. A compromised SDN controller can grant adversaries extensive control over traffic routing, policy enforcement, and network orchestration. Consequently, strong authentication, encrypted control channels, controller redundancy, and continuous monitoring are essential to securing SDN environments (Cisco Systems, 2023).

2.2 Network Function Virtualization (NFV)

Network Function Virtualization replaces dedicated hardware appliances with software-based virtual network functions (VNFs) deployed on commodity computing platforms. Common VNFs include virtual firewalls, virtual intrusion detection systems, virtual load balancers, and virtual evolved packet cores. NFV reduces operational costs and accelerates service deployment while enabling flexible service chaining and resource allocation. However, virtualization introduces unique security challenges. Attackers may exploit hypervisor vulnerabilities to perform virtual machine escape attacks, thereby compromising host systems and neighboring VNFs. Additional threats include resource exhaustion attacks, malicious virtual machine migration, and insecure orchestration pipelines. Therefore, securing virtualized infrastructure requires hypervisor hardening (ETSI, 2021)., secure orchestration, access control enforcement, and continuous vulnerability assessment.

2.3 Edge Computing Security

Edge computing pushes computational resources closer to end devices (Shi et al., 2016)., reducing latency and improving real-time responsiveness. This architecture is particularly important for latency-sensitive applications such as autonomous

vehicles, industrial robotics, and remote healthcare systems. However, distributing computation across edge nodes increases the attack surface by exposing more endpoints to potential compromise. Edge nodes may be vulnerable to physical tampering, unauthorized access, malware injection, and side-channel attacks. Since these nodes often operate in distributed and less controlled environments, robust edge security protocols, device authentication, and zero-trust access models become essential for maintaining system integrity. The proposed security framework introduces several innovations for securing next-generation wireless environments:

- Lightweight integrity checks using wireless telemetry parameters such as Received Signal Strength Indicator (RSSI) and Channel Quality Indicator (CQI) for context-aware anomaly detection.
- Shapley Additive Explanations (SHAP)-driven drift monitoring to detect ML model degradation before performance decline.
- Quantum-safe application programming interfaces (APIs) integrated with zero-trust security enforcement.
- Blockchain-based model provenance to ensure tamper-resistant audit trails for intrusion detection model updates.

The vision for 6G extends beyond incremental network improvements toward ubiquitous intelligence, autonomous orchestration, and integrated terrestrial–non-terrestrial communications involving satellites, aerial platforms, and ground infrastructure. Security in 6G must address challenges across multiple dimensions. First, data security and privacy become critical due to the large-scale integration of IoT devices and user-generated data, necessitating privacy-preserving analytics and secure federated learning. Second, AI/ML security emerges as a major concern because AI will serve as a core operational component of 6G systems, making adversarial machine learning attacks such as poisoning and evasion particularly dangerous. Third, cross-domain security becomes increasingly complex due to heterogeneous communication environments involving terrestrial, aerial, and satellite segments. Finally, quantum threats challenge conventional cryptographic systems, necessitating the adoption of post-quantum cryptographic mechanisms.

Securing these dynamic wireless environments requires adaptive security frameworks capable of real-time threat detection, automated mitigation, and continuous learning. Rigorous certification of SDN controllers, NFV hypervisors, edge nodes, and AI models will be critical for building trustworthy and resilient future wireless communication systems. Thus, the transition from 4G to 5G and eventually to 6G represents not merely a technological upgrade but a fundamental redefinition of networking paradigms and associated security requirements (European Commission, 2024).

3. Machine Learning Techniques and Comparative Overview Against Established Intrusion Detection Methods

Machine learning (ML) has emerged as a highly effective approach for detecting complex intrusions and anomalies in modern wireless networks. Unlike conventional rule-based intrusion detection systems that depend heavily on predefined signatures, ML-based systems possess the capability to learn from network traffic patterns, identify anomalies, and adapt to evolving cyber threats. This adaptability makes ML particularly suitable for 5G and emerging 6G environments characterized by dynamic traffic patterns, large-scale device heterogeneity, and increasingly sophisticated attack surfaces (Shafiq et al., 2020).

The effectiveness of ML-based intrusion detection systems is largely determined by the choice of learning algorithm, feature engineering strategies, and the quality of training datasets. Different ML paradigms offer unique strengths for specific intrusion detection scenarios, ranging from detecting known attack signatures to identifying zero-day exploits and optimizing adaptive defense mechanisms.

3.1 Supervised Learning

Supervised learning algorithms are trained using labeled datasets containing both benign and malicious network traffic. These models learn to classify traffic patterns based on historical attack signatures and are highly effective in detecting known threats such as denial-of-service (DoS), distributed denial-of-service (DDoS), spoofing, and malware propagation. Popular supervised learning algorithms include Random Forest, Support Vector Machines (SVM), Decision Trees, Gradient Boosting, and XGBoost. These models often achieve high classification accuracy due to their ability to exploit labeled attack datasets. Random Forest, for example, is widely used (Breiman, 2001; Bishop, 2006). because of its robustness against overfitting and strong performance in high-dimensional data environments. Despite their effectiveness, supervised models require large, well-labeled datasets, which are often difficult and expensive to obtain in real-world wireless environments. Furthermore, these models generally struggle to detect previously unseen or zero-day attacks since they are biased toward known traffic patterns (Bharati et al., 2021).

3.2 Unsupervised Learning

Unsupervised learning techniques analyze unlabeled data to identify hidden structures or abnormal behaviors within network traffic. These methods are particularly valuable for detecting zero-day attacks and previously unknown anomalies where labeled attack data is unavailable. Common unsupervised learning algorithms include K-Means clustering, Isolation Forests, Principal Component Analysis (PCA), and Autoencoders. These algorithms establish a baseline of normal network behavior and flag deviations as suspicious activities. For instance, Isolation Forests effectively isolate anomalous samples (Liu et al., 2008; Chandola et al., 2009), by recursively partitioning data points, making them suitable for large-scale anomaly detection in wireless networks. The major advantage of unsupervised learning lies in its ability to identify

unknown threats in dynamic environments. However, these techniques often produce higher false-positive rates because legitimate traffic variations may be incorrectly classified as malicious. This remains a significant challenge in highly dynamic 5G and 6G communication environments.

3.3 Reinforcement Learning

Reinforcement learning (RL) offers a powerful framework for adaptive threat response and autonomous decision-making in cybersecurity. In RL-based intrusion detection, an intelligent agent learns optimal defense strategies (Sutton & Barto, 2018). by interacting with the network environment and receiving rewards or penalties based on its actions. Algorithms such as Q-Learning and Deep Q-Networks (DQN) enable security systems to dynamically optimize responses such as traffic filtering, node isolation, bandwidth throttling, or rerouting malicious flows. This approach is particularly useful in rapidly changing wireless environments where static response policies may become ineffective. One of the major strengths of reinforcement learning is its ability to continuously improve defense strategies over time. However, RL models often suffer from slow convergence and exploration-exploitation trade-offs, especially in large-scale real-world deployments with complex state spaces.

3.4 Deep Learning Architectures

Deep learning has significantly enhanced intrusion detection by enabling automatic extraction of complex hierarchical features from raw network traffic data. Unlike traditional ML methods that require manual feature engineering, deep neural networks can learn intricate patterns directly from large datasets. Common deep learning architectures used in wireless intrusion detection include:

- Convolutional Neural Networks (CNNs): Effective for extracting spatial features and traffic correlations.
- Recurrent Neural Networks (RNNs): Suitable for sequential traffic analysis and temporal pattern recognition.
- Long Short-Term Memory (LSTM): Highly effective in detecting temporal dependencies in network behavior.
- Transformers: Capable of modeling long-range dependencies (Vaswani et al., 2017). in large-scale traffic datasets.
- Graph Neural Networks (GNNs): Useful for analyzing communication relationships among interconnected devices.

Deep learning models demonstrate superior performance in detecting sophisticated attacks such as botnets, advanced persistent threats (APTs), and coordinated multi-vector attacks. Recent studies have proposed hybrid deep reinforcement learning models that combine Multi-Layer Perceptrons (MLP), CNNs, and optimized recurrent neural networks to improve detection accuracy in IoT-based wireless environments (Aloqaily et al., 2021; Goodfellow et al., 2016). However, deep learning approaches face challenges including high computational complexity, energy consumption, training cost, and limited explainability due to their black-box nature.

3.5 Layer-Oriented Threat Telemetry

An advanced perspective on intrusion detection involves mapping ML sensors to specific layers of wireless network architecture. This layer-oriented telemetry enhances contextual threat visibility and improves detection precision. Examples include:

- Physical-layer anomaly detectors: Monitor signal behavior, radio interference, RSSI fluctuations, and spectrum anomalies.
- Control-plane detectors: Analyze SDN controller flow logs, slice orchestration messages, and policy updates.
- Service-layer detectors: Inspect API traces, HTTP/2 transactions, gRPC headers, container logs, and orchestration events.
- Application-layer detectors: Identify malicious user behavior, access abuse, and abnormal service requests.

This multi-layer telemetry approach enables comprehensive monitoring across heterogeneous 5G and 6G infrastructures.

3.6 Comparative Overview of ML Techniques

Table 1 presents a comparative overview of major machine learning approaches used for intrusion detection and prevention in 5G and future 6G networks.

Overall, no single ML technique is universally optimal for all intrusion detection scenarios. Hybrid approaches that combine supervised, unsupervised, and reinforcement learning techniques often provide the best balance between detection accuracy, adaptability, and operational efficiency. Such hybrid architectures are expected to become central to future 6G security frameworks.

Table 1: Major machine learning approaches used for intrusion detection and prevention

ML Technique	**Purpose**	**Advantages**	**Challenges**
Supervised Learning (Random Forest, XGBoost)	Classify known attacks using labeled data	High accuracy for known threats	Requires labeled datasets; poor zero-day detection
Unsupervised Learning (K-Means, Isolation Forest, Autoencoders)	Detect anomalies without labels	Effective against unknown threats	High false positives
Reinforcement Learning (Q-Learning, DQN)	Adaptive threat response	Dynamic defense optimization	Slow convergence
Deep Learning (CNN, RNN, LSTM, Transformers)	Automatic feature extraction	Handles complex large datasets	High computational cost; explainability issues

4. Proposed Methodology and Wireless Intrusion Detection Algorithm (WIDA)

Machine learning provides a robust and intelligent approach for detecting both known and emerging security threats in wireless communication networks. A reliable intrusion detection and prevention framework begins with the collection of relevant data from multiple sources, including wireless network traffic, telemetry streams, system logs, and network management platforms. The quality, diversity, and representativeness of these datasets significantly influence the effectiveness and generalization capability of machine learning models used for intrusion detection (Bharati et al., 2021).

4.1 Data Collection and Preprocessing

The first stage of the proposed methodology involves acquiring large-scale network data from heterogeneous wireless environments such as base stations, edge nodes, IoT devices, and core network components. The collected data typically contain raw traffic records, packet metadata, signaling information, wireless channel measurements, and system event logs. Following data collection, preprocessing is performed to improve data quality and ensure consistency for machine learning analysis. Preprocessing operations include:

- Data cleaning to remove incomplete, duplicated, or corrupted records
- Normalization to scale feature values within comparable ranges
- Noise reduction to improve signal quality
- Feature extraction to derive meaningful security indicators
- Dimensionality reduction to reduce computational complexity

Effective preprocessing improves model accuracy, convergence speed, and overall detection reliability.

4.2 Feature Engineering

Feature engineering plays a crucial role in enhancing model performance by identifying the most informative attributes from the collected data. Carefully selected features improve the model's ability to distinguish between benign and malicious activities. Relevant security features may include:

- Packet size distribution
- Protocol type
- Flow duration
- Source and destination IP behavior
- Traffic burst patterns
- Signal strength indicators (RSSI)
- Channel Quality Indicator (CQI)
- User mobility behavior
- Frequency spectrum utilization
- Authentication request frequency

These engineered features enable more accurate detection of subtle attack behaviors such as spoofing, botnet propagation, signaling abuse, and DDoS attacks.

4.3 Model Training and Evaluation

After preprocessing and feature engineering, the dataset is divided into training and testing subsets. The training dataset is used to build machine learning models capable of learning patterns associated with both normal and malicious network behavior, while the testing dataset evaluates model performance on unseen data.

Depending on the application scenario, one or more ML paradigms may be employed:

- Supervised learning for known attack classification
- Unsupervised learning for anomaly detection
- Reinforcement learning for adaptive defense optimization
- Deep learning for complex pattern recognition

Performance evaluation metrics commonly include:

- Accuracy
- Precision
- Recall
- F1-score
- False Positive Rate (FPR)
- Detection latency

These metrics provide quantitative measures of intrusion detection effectiveness and operational efficiency.

4.4 Real-Time Intrusion Detection and Prevention Framework

Once trained, the machine learning model is integrated into a real-time intrusion detection and prevention system (IDPS). The deployed framework continuously monitors live network activities and analyzes incoming traffic streams for suspicious behaviors. When anomalies or malicious patterns are detected, the system automatically initiates mitigation responses such as:

- Traffic filtering
- Connection termination
- Malicious node isolation
- Dynamic rerouting
- Access restriction
- Security alert generation

This automated response capability significantly reduces incident response time and improves network resilience.

4.5 Explainable Artificial Intelligence (XAI)

To improve trust, transparency, and operational confidence in ML-driven security systems, Explainable Artificial Intelligence (XAI) techniques are incorporated into the framework. XAI provides interpretable insights into model decisions, allowing administrators to understand why specific traffic patterns are classified as malicious. This is especially important in critical infrastructures such as telecommunications, where explainability supports:

- Regulatory compliance
- Security auditing
- Operator trust
- Incident investigation
- Model debugging and refinement

Techniques such as SHAP (Shapley Additive Explanations) (Lundberg & Lee, 2017). help quantify feature importance and improve interpretability of complex models.

4.6 Wireless Intrusion Detection Algorithm (WIDA)

The proposed Wireless Intrusion Detection Algorithm (WIDA) is designed to strengthen security in 5G and future 6G networks by combining machine learning-based anomaly detection with adaptive prevention mechanisms. WIDA enables continuous monitoring, automated response, and model adaptation to emerging threats. Its major objective is to improve detection accuracy while minimizing false positives and false negatives.

Algorithm Steps

1. Input network traffic data, wireless telemetry, and system logs.
2. Preprocess and normalize the collected data.
3. Extract critical security-related features.
4. Train ML model using historical benign and attack data.
5. Continuously monitor live traffic streams.
6. Detect deviations from normal behavior.
7. Classify anomalies as benign or malicious.
8. Trigger automated mitigation responses.

9. Update model periodically using new threat intelligence.

Pseudocode for WIDA

```
Begin WIDA
  Input network_data
  Preprocess network_data
  Extract security_features
  Train ML_model using training_data
  While network is active do
    Capture incoming_traffic
    Extract features
    anomaly_score = ML_model.predict(features)
    If anomaly_score > threshold then
      Classify attack_type
      Trigger mitigation_response
      Log incident
    Else
      Continue monitoring
    End If
  End While
  Periodically retrain ML_model using updated_data
End WIDA
```

The feedback mechanism ensures that WIDA remains adaptive to emerging attack patterns and evolving wireless network behaviors. By incorporating continuous learning, the framework improves detection accuracy over time while reducing operational blind spots.

4.7 Architecture of the Proposed WIDA Framework

The WIDA architecture consists of six major layers:

4.7.1 Data Acquisition Layer

Collects network traffic, wireless telemetry, and system logs from base stations, edge nodes, IoT devices, and core infrastructure.

4.7.2 Preprocessing Layer

Cleans, normalizes, and transforms raw data into structured machine-readable inputs.

4.7.3 Feature Engineering Layer

Extracts security-relevant features such as packet behavior, signal quality, and traffic statistics.

4.7.4 ML Detection Engine

Applies trained machine learning models to classify traffic patterns and detect anomalies in real time.

4.7.5 Decision and Response Layer

Executes mitigation strategies including blocking malicious traffic, isolating compromised nodes, rerouting flows, and generating alerts.

4.7.6 Continuous Learning Layer

Updates model parameters using newly observed threat intelligence and feedback from previous detections. This layered architecture provides an adaptive, scalable, and intelligent security framework capable of protecting next-generation wireless communication infrastructures against evolving cyber threats.

5. Implementation and Real-World Case Studies

The practical implementation of machine learning-based intrusion detection and prevention systems in 5G and emerging 6G environments demonstrates the viability of adaptive security mechanisms in real-world wireless deployments. As cyber threats become increasingly sophisticated, telecommunication operators, research institutions, and industrial organizations are adopting artificial intelligence-driven security solutions to improve the protection of critical communication infrastructures.

Real-world deployment of ML-driven security systems highlights their ability to enhance detection accuracy, reduce response time, and support automated threat mitigation across large-scale wireless ecosystems. These implementations also demonstrate how adaptive security models can effectively address evolving attack patterns that conventional rule-based systems often fail to detect.

5.1 Smart City IoT Security Deployment

One notable implementation involves the deployment of deep learning-based intrusion detection systems in smart city Internet of Things (IoT) ecosystems. Smart cities rely heavily on interconnected devices such as sensors, surveillance cameras, traffic management systems, and intelligent utility infrastructures that continuously exchange data over 5G networks. Traditional rule-based security systems often struggle to identify dynamic threats such as botnet activities, spoofing attacks, unauthorized access attempts, and distributed denial-of-service (DDoS) attacks in such highly connected environments. By deploying deep neural networks trained on large-scale traffic datasets, researchers achieved significantly improved detection performance with reduced false alarm rates. The ML-based system successfully identified malicious traffic patterns in near real time, enabling faster mitigation of coordinated cyberattacks. This deployment demonstrated how deep learning models can improve resilience and maintain service availability in highly complex urban communication infrastructures (Shafiq et al., 2020).

5.2 Edge Computing Security Implementation

Another important real-world implementation is found in edge computing environments, where intrusion detection models are deployed directly at edge nodes rather than centralized cloud servers. Edge-based security architectures are particularly valuable in latency-sensitive applications such as autonomous driving, industrial automation, smart manufacturing, and remote medical systems. Deploying intrusion detection at edge nodes reduces latency and enables faster decision-making closer to data sources. This architecture improves responsiveness and minimizes the delay associated with centralized analysis. For example, an ML-enabled edge intrusion detection system used in autonomous vehicle communication networks demonstrated strong performance in detecting anomalies in:

- Vehicle-to-Vehicle (V2V) communication
- Vehicle-to-Infrastructure (V2I) communication
- Edge-to-Cloud communication

The system employed reinforcement learning to dynamically adjust mitigation strategies based on attack severity, traffic conditions, and network state. This adaptive response mechanism significantly improved security resilience and reduced incident response time (Aloqaily et al., 2021).

5.3 Federated Learning for Privacy-Preserving Security

Telecommunication service providers are increasingly exploring federated learning as a privacy-preserving approach for collaborative intrusion detection. Instead of transmitting raw network traffic data to centralized servers, federated learning enables local machine learning models to be trained independently at distributed nodes such as base stations, edge devices, or regional network clusters. Only model parameters or learned updates are shared with a central aggregator, thereby preserving user privacy while enabling collaborative intelligence across multiple network domains. This approach provides several benefits:

- Improved privacy protection
- Reduced centralized data exposure
- Regulatory compliance
- Better scalability for distributed infrastructures
- Enhanced resilience to localized attacks

Federated intrusion detection is particularly promising for future 6G environments, where decentralized intelligence and autonomous orchestration are expected to become fundamental operational requirements (Nguyen et al., 2022).

5.4 Practical Benefits of ML-Based Security Systems

The examined case studies reveal several major advantages of machine learning-based intrusion detection and prevention systems in wireless environments:

5.4.1 Improved Detection Accuracy

ML models can recognize complex patterns that traditional systems may overlook, leading to more accurate identification of cyber threats.

5.4.2 Faster Response Time

Real-time analysis and automated mitigation significantly reduce the time between attack detection and response.

5.4.3 Scalability

ML-based systems efficiently handle massive traffic volumes generated by 5G and future 6G networks.

5.4.4 Adaptive Threat Intelligence

Continuous learning enables systems to adapt to new attack strategies and previously unseen threats.

5.4.5 Reduced Human Intervention

Automated anomaly detection and response decrease dependence on manual security operations.

5.5 Implementation Challenges

Despite these advantages, practical deployment of ML-based security systems presents several challenges.

5.5.1 Model Explainability

Complex deep learning models often behave as black boxes, making it difficult for administrators to interpret security decisions.

5.5.2 Computational Overhead

Advanced ML models may require substantial processing power, memory, and energy, particularly in edge environments.

5.5.3 Adversarial Attacks

Attackers may intentionally manipulate input data or training datasets to deceive ML models.

5.5.4 Secure Model Lifecycle Management

Model updates, retraining, and deployment pipelines must be protected against tampering and unauthorized modifications. These challenges emphasize the need for robust governance frameworks, explainable AI techniques, and secure model management practices. Overall, real-world implementations demonstrate that machine learning-based adaptive intrusion detection systems offer substantial improvements in detection capability, scalability, and automated response. However, their successful deployment requires addressing operational, computational, and security challenges associated with AI-driven systems.

6. Challenges and Future Research Directions

Despite the significant promise of machine learning in strengthening wireless network security, several critical challenges remain unresolved. While ML-driven intrusion detection and prevention systems have demonstrated strong capabilities in anomaly detection, adaptive response, and intelligent threat mitigation, their large-scale deployment in 5G and emerging 6G networks continues to face technical, operational, and regulatory obstacles.

6.1 Dataset Scarcity and Data Quality

One of the most significant challenges in machine learning-based intrusion detection is the availability of high-quality datasets for model training and evaluation. Many publicly available cybersecurity datasets do not accurately represent real-world 5G and future 6G traffic characteristics, particularly in highly dynamic and heterogeneous environments involving IoT devices, edge computing platforms, network slicing, and virtualized network functions. This lack of representative data negatively affects model generalization and may lead to reduced detection accuracy when deployed in operational environments. Furthermore, data imbalance between normal and attack traffic often introduces bias during training, causing models to favor majority classes while underperforming on rare but critical attack types. Future research should focus on the development of realistic, large-scale, and continuously updated benchmark datasets tailored specifically for 5G and 6G security applications (Bharati et al., 2021).

6.2 Model Explainability and Trustworthiness

Another major challenge is the explainability of machine learning models, particularly deep learning architectures. Many high-performing models operate as black boxes, making it difficult for network administrators and security analysts to understand the reasoning behind detection decisions. In critical infrastructures such as telecommunications, explainability is essential for:

- Accountability
- Security auditing
- Regulatory compliance
- Incident analysis
- Operator trust

Without interpretable insights, false positives or false negatives may be difficult to investigate and resolve. Explainable Artificial Intelligence (XAI) techniques, such as SHAP and Local Interpretable Model-Agnostic Explanations (LIME), offer promising solutions for improving transparency. However, balancing model complexity, performance, and interpretability remains an open research challenge.

6.3 Adversarial Machine Learning Attacks

Adversarial machine learning represents one of the most serious threats to AI-driven security systems. Attackers can intentionally manipulate training data or craft malicious input samples to deceive ML models and force incorrect predictions.

Two major forms of adversarial attacks include:

6.3.1 Data Poisoning Attacks

Attackers inject manipulated or malicious samples into training datasets to corrupt the learning process.

6.3.2 Evasion Attacks

Attackers craft specially designed inputs that appear normal to the model but contain malicious intent. Such attacks can degrade detection performance, create security blind spots, and compromise automated defense systems. Therefore, future intrusion detection frameworks must incorporate adversarial robustness and resilient learning strategies to withstand malicious manipulation (Goodfellow et al., 2016).

6.4 Computational Complexity and Energy Consumption

Advanced machine learning models—particularly deep neural networks—often require substantial computational resources, memory capacity, and energy consumption. This presents a significant challenge for edge-based intrusion detection in resource-constrained environments such as IoT devices, mobile edge nodes, and embedded communication systems.

High computational overhead may lead to:

- Increased inference latency
- Higher energy consumption
- Reduced battery life
- Limited scalability in distributed systems

Future research should prioritize lightweight yet accurate machine learning models optimized for low-power, real-time wireless environments. Techniques such as model compression, pruning, quantization, and edge-specific acceleration will become increasingly important.

6.5 Regulatory and Privacy Challenges

As AI becomes more deeply integrated into critical infrastructures, compliance with legal and regulatory frameworks becomes increasingly important. Regulations such as the European Union Artificial Intelligence Act impose strict requirements on high-risk AI systems, including those used in telecommunications and cybersecurity.

These requirements include:

- Transparency in automated decision-making
- Bias mitigation
- Secure lifecycle management
- Human oversight
- Accountability mechanisms

Privacy preservation also remains a central concern, especially in systems handling sensitive user communications and behavioral data. Privacy-preserving learning techniques such as federated learning, secure multiparty computation, and differential privacy are expected to play key roles in future wireless security frameworks (European Commission, 2024; Nguyen et al., 2022).

6.6 Future Research Directions

Future 6G security architectures are expected to evolve toward highly autonomous, self-learning defense ecosystems capable of detecting, predicting, and neutralizing threats with minimal human intervention. Promising research directions include:

6.6.1 Self-Learning Autonomous Defense Systems

Future security systems will increasingly leverage autonomous AI agents capable of proactive threat hunting and adaptive response.

6.6.2 Quantum-Resistant Cryptography

The emergence of quantum computing threatens conventional cryptographic methods. Post-quantum cryptographic mechanisms will become essential for future wireless security.

6.6.3 Federated and Collaborative Intelligence

Distributed learning frameworks will enable secure collaborative intrusion detection without compromising user privacy.

6.6.4 Neuromorphic Computing

Brain-inspired computing architectures may enable ultra-efficient AI inference for low-power edge security applications.

6.6.5 Blockchain-Based Trust Management

Blockchain technology can provide tamper-resistant audit trails, secure model provenance, and decentralized trust management.

6.6.6 Digital Twin Security Modeling

Digital twins of communication networks may enable simulation-based threat prediction and proactive defense testing before real-world deployment. In summary, while machine learning offers transformative opportunities for securing future

wireless networks, addressing challenges related to dataset quality, explainability, adversarial robustness, computational efficiency, and regulatory compliance remains essential. Overcoming these barriers will be critical for building resilient, trustworthy, and intelligent 6G security ecosystems.

7. Conclusion

The transition from fifth-generation (5G) to future sixth-generation (6G) wireless networks introduces unprecedented opportunities for ultra-fast, intelligent, and highly interconnected communication systems. However, this transformation also significantly broadens the attack surface, exposing wireless infrastructures to increasingly sophisticated and dynamic cyber threats. Conventional security mechanisms alone are no longer sufficient to address the complexity and scale of these emerging security challenges. This paper presented a comprehensive review of machine learning approaches for adaptive intrusion detection and prevention in 5G and future 6G networks. Various machine learning paradigms—including supervised learning, unsupervised learning, reinforcement learning, and deep learning—were examined based on their capabilities, strengths, and limitations in wireless security applications. A novel Wireless Intrusion Detection Algorithm (WIDA) was proposed as an adaptive security framework that integrates real-time anomaly detection, automated mitigation, and continuous learning. The proposed framework demonstrates how ML-driven security systems can significantly improve detection accuracy, reduce response latency, and enhance resilience against evolving cyber threats. Furthermore, real-world case studies highlighted the practical feasibility of deploying intelligent intrusion detection systems in smart city infrastructures, edge computing environments, and privacy-preserving federated learning architectures. Despite these advancements, several critical challenges remain, including dataset scarcity, model explainability, adversarial attacks, computational overhead, and regulatory compliance. These challenges present significant barriers to large-scale deployment and require continued research attention. Future research should prioritize the development of lightweight, explainable, robust, and quantum-resistant security mechanisms capable of supporting autonomous defense in 6G ecosystems. Emerging technologies such as federated learning, blockchain-enabled trust management, post-quantum cryptography, and neuromorphic computing are expected to play essential roles in shaping next-generation wireless security. In conclusion, machine learning will remain a foundational technology in the evolution of wireless cybersecurity. By integrating adaptive intelligence with advanced intrusion detection and prevention mechanisms, future communication networks can achieve improved trustworthiness, resilience, scalability, and operational security.

References

3rd Generation Partnership Project. (2023). *TS 33.501: Security architecture and procedures for 5G systems*.

Aloqaily, M., Otoum, S., Ridhawi, I. A., & Jararweh, Y. (2021). An intrusion detection system for connected vehicles in smart cities using machine learning. *Journal of Network and Computer Applications*.

Andrews, J. G., et al. (2014). What will 5G be? IEEE Journal on Selected Areas in Communications, 32(6), 1065–1082.

Bharati, A., Benedetto, F., & Mazzenga, F. (2021). Data collection and preprocessing for wireless intrusion detection using machine learning: A systematic approach. *Sensors*.

Bishop, C. M. (2006). Pattern recognition and machine learning. Springer.

Breiman, L. (2001). Random forests. Machine Learning, 45(1), 5–32.

Chandola, V., Banerjee, A., & Kumar, V. (2009). Anomaly detection: A survey. ACM Computing Surveys, 41(3), 1–58.

Cisco Systems. (2023). *Annual cybersecurity report: Emerging threats in 5G infrastructure*. Cisco.

ETSI. (2021). Network Functions Virtualisation (NFV): Security.

European Commission. (2024). *Artificial Intelligence Act: Regulatory framework for AI in the European Union*. European Union.

Goodfellow, I., Bengio, Y., & Courville, A. (2016). *Deep learning*. MIT Press.

Kreutz, D., et al. (2015). Software-defined networking: A comprehensive survey. Proceedings of the IEEE, 103(1), 14–76.

Liu, F. T., Ting, K. M., & Zhou, Z. H. (2008). Isolation forest. ICDM.

Lundberg, S. M., & Lee, S. I. (2017). A unified approach to interpreting model predictions. NeurIPS.

Nguyen, T. T., Reddi, V. J., & Kumar, S. (2022). Federated learning for secure wireless communication networks. *IEEE Communications Surveys & Tutorials*.

Shafiq, M., Tian, Z., Bashir, A. K., Jolfaei, A., & Yu, X. (2020). Data mining and machine learning methods for cyber security intrusion detection: A survey. *IEEE Access*.

Shi, W., et al. (2016). Edge computing: Vision and challenges. IEEE Internet of Things Journal, 3(5), 637–646.

Sommer, R., & Paxson, V. (2010). Outside the closed world: On using machine learning for network intrusion detection. IEEE Symposium on Security and Privacy.

Sutton, R. S., & Barto, A. G. (2018). Reinforcement learning: An introduction (2nd ed.). MIT Press.

Vaswani, A., et al. (2017). Attention is all you need. NeurIPS.