International Journal for Multidisciplinary Research (IJFMR)
E-ISSN: 2582-2160 ● Website: www.ijfmr.com ● Email: editor@ijfmr.com

Optimizing Anomaly Detection in 5G and Beyond Networks using Reinforcement Learning

Benson Mbithi[1], Bernard Ondara[2]

[1,2]Department of Computing and Information Technology, Kenyatta University, Kenya

Abstract

Kenya has experienced significant growth in internet use and adoption, evidenced by the rapid deployment of 5G networks. Cyberthreats' sophistication, coupled with 5G network complexity, has increased the risk of security problems. Anomaly detection tools developed for earlier generations of networks are ineffective for 5G and beyond networks, and cannot learn and adapt from interactions with their environment. This study investigates current anomaly detection techniques in 5G networks in local Network Facility Providers in Kenya, evaluates their performance, and develops a reinforcement learning-based model using the 5G-NIDD dataset for improved anomaly detection. A structured questionnaire was distributed online to 29 network management professionals across 11 Network Facility Providers in Kenya, using convenience and purposive sampling. The responses were analyzed using descriptive statistics and thematic analysis to achieve study objectives. The results revealed that most local providers used commercial solutions for anomaly detection, which are rule-based or signature-driven. A Deep Q-Network reinforcement learning model was designed and trained to classify benign and eight types of network attacks using the 5G NIDD dataset. Experimental results showed significant improvement in detection performance, achieving an overall accuracy of 75.41% after refinement. This study confirms the potential of reinforcement learning to address critical limitations in existing solutions and provides a promising direction for enhancing the security resilience of 5G and beyond networks.

Keywords: Reinforcement learning, Deep Q-learning, 5G networks, anomaly detection, Network Facility providers, Network Anomalies, 5G-NIDD dataset.

1. Introduction

Kenya has experienced significant growth in internet use and adoption, as evidenced by an increase in mobile subscriptions, data/internet subscriptions, traffic, and international bandwidth. The total mobile data subscriptions as of September 2025 stood at 60.2 million, out of which 2.4%, representing 1,496,799 subscribers, were on the fifth-generation (5G) network (Communications Authority of Kenya, 2025). Additionally, the report highlights that data consumption among 4G and 5G users grew significantly from September 2024 to September 2025, whereas 3G declined following a shift in consumer preference for higher and faster internet speeds.

The Internet has enabled the sharing of information resources among people, facilitating their work and lives, and has made them increasingly inseparable from the Internet. This rapid growth has created a pressing demand for the deployment of 5G networks to accommodate the high data traffic and improve connectivity speeds. 5G networks' ability to simultaneously support multiple connections, minimal latency

and high capacity (Goswami & Choudhury, 2022), has emerged as an effective tool for modern digital communication.

This digital growth is not without its challenges. This technological evolution has given rise to complexities in the domain of 5G network management. 5G networks are susceptible to various cyberattacks and security risks. The rapid advancement and adoption of 5G networks in Kenya (Communication Authority of Kenya, 2025) have led to an increase in the number of internet users, which has led to an increase in the number of connections and an increase in 5G traffic. The large amount of data generated by 5G networks (Alanazi, 2023) and the rise in the number of internet-connected devices that can potentially induce vulnerability (Goswami & Choudhury, 2022) have made network management more complex and increased the risk of security problems. Coupled with the increasing complexity, sophistication, and diversity of network infrastructures (Deepika et al., 2024a), cyber threats incidents have increased. According to the Communication Authority (CA) of Kenya, the Computer Incident Response Team Coordination Center (CIRT/CC) detected 842 million cyber threat events for the period between July and September 2025 (Communication Authority of Kenya, 2025). The majority of the attacks targeted organizations within the Information Communication Technology (ICT) sector and Internet Service Providers (ISPs), cloud solutions providers, and health service providers reported the highest number of system attacks. Tools developed for the 3 G and 4 G generation networks are ineffective for 5G networks due to the variation in application areas, standards, and data rates. Traditional signature-based detection has been proposed and used (Rahman et al., 2022). However, these methods require prior information for anomalies to be detected which is unsuitable against newly emerging or previously unseen patterns that may not yet have corresponding labels. (Bouke & Abdullah, 2024) proposed the use of supervised and unsupervised learning-based techniques. Despite them being a great tool to introduce intelligence to network management, they cannot learn from interactions with their environment. Therefore, there is a need for a technique that interacts with its environment to learn and adapt to dynamic network conditions.

Characterized by their capacity to make sequences of decisions and learn optimal policies through trial and error, Reinforcement Learned (RL) techniques can interact with their environment to learn and adapt to dynamic network conditions. Despite their potential, the application of RL in cybersecurity remains underexplored (Ahmadi & Chen, 2024), particularly in the context of 5G and beyond networks. The study aims to optimize anomaly detection accuracy in 5G networks using the Deep Q algorithm, utilizing the 5G-Non-IP Data Delivery (NIDD) dataset.

2. Related Literature

According to (Ghafir et al., 2015), network monitoring enables network administrators to know the instantaneous state of a computer network. It can assess the usage of diverse resources, traffic flows and performance-related parameters such as latency, throughput, packet loss, and signal. ISPs facilitate access to the Internet and associated services. They oversee network traffic, helping to manage and track performance metrics such as latency, bandwidth utilization and signal quality. They also assist in detecting abnormal behavior from potential attackers and mitigating anomalies within the network.

The Communications Authority (CA) of Kenya is mandated to license network facility providers. CA categorizes the Network Facility Providers in a tiered system, Tier 1, 2 and 3, distinguishing the scope of their services. Tier 1 serves as the backbone of the global infrastructure. They are top-level and operate on a worldwide scale and supply connectivity to other low-level tiers. Examples in Kenya include

Safaricom Plc, Airtel Networks Kenya Limited, Jamii Telecommunications and Telkom Kenya Limited (Communications Authority of Kenya, 2025). Tier 2 ISPs operate on a national or regional level and rely on Tier 1 ISPs for global reach. Some of the Tier 2 ISPs in Kenya include Kenya Education Network, Liquid Intelligent Technologies, Kenya Pipeline Company Limited, Kenya Electricity Transmission Company Limited, Vodacom Business Kenya Limited and Kenya Power and Lighting Company PLC (Communications Authority of Kenya, 2025). Tier 3 ISPs provide internet access to end users. Examples in Kenya include Adrian Kenya Limited, Fimnet Communications Limited, and Nextgen Networks Limited (Communications Authority of Kenya, 2025).

According to the CA of Kenya, cyberattack incidents have significantly increased. During the period between July and September 2025, the National KE-CIRT/CC detected 842.3 million cyberthreat events, as shown in Table 1 below. The majority of the attacks targeted organizations within the Information Communication Technology (ICT) sector, and ISPs, cloud solutions providers, and health service providers reported the highest number of system attacks.

Table 1: Cyber Security Threat Landscape in Kenya Source National KE_CIRT/CC

S/No	Threats	July-September 2025	April- June 2025	January-March 2025	October-December 2024
1	Malware	31,676,444	47,397,554	24,549,413	33,920,406
2	Brute Force Attack	18,811,738	20,947,973	33,794,288	34,784,028
3	Web Application Attacks	10,417,253	12,742,473	5,081,236	4,542,939
4	System vulnerabilities	776,542,757	4,492,325,076	2,470,257,079	752,441,233
5	Mobile Application Attacks	76,891	189,004	68,063	138,175
6	DDOS	4,795,584	13,080,197	3,678,789	15,095,217
Totals Cyber Threats		**842,320,667**	**4,586,682,277**	**2,537,428,868**	**840,921,998**

The majority of the attacks targeted organizations within the Information Communication Technology (ICT) sector, and ISPs, cloud solutions providers, and health service providers reported the highest number of system attacks.

Cyberattacks are initially characterized by anomalies that disrupt the baseline behavior of a system. In network traffic, an anomaly is anything that causes unusual and significant changes in network behavior. Anomalies in networks may manifest as sudden spikes in traffic, unusual patterns in signal strength, or unexpected device behaviors (Deepika et al., 2024a). Anomalies introduce security vulnerabilities, allowing for potential attacks that further strain network resources, degrading the overall quality of 5G network services. Anomalies in network traffic arise from various activities in networks such as malware and cybercrime activities. These anomalies could indicate potential security threats in network traffic. Threats in 5G networks can arise from multiple sources, including malicious actors, vulnerabilities in enabling technologies, and entry points in network architectures (Tariq et al., 2024).

Failure to detect anomalies on time can compromise network integrity, straining network resources and, in extreme cases, leading to a surge in security incidents that may affect network availability, CPU, and memory utilization, degrading 5G services (Lam & Abbas, 2020). The identification of these unusual patterns has proven to be a powerful tool across numerous domains such as computer networks, industrial processes, medical diagnosis and fraud detection. Anomaly detection is founded on establishing a baseline profile for normal activity (Ahmad et al., 2021) and deviation from this baseline profile is identified as an anomaly. Anomaly detection functions as an early-warning mechanism, spotting irregular behaviors in network traffic that might point to security vulnerabilities. The ability to quickly and accurately detect anomalies is essential in 5G environments, where even minor network disruptions can lead to large-scale service outages, security vulnerabilities, and increased operational costs.

Anomaly intrusion detection has attracted a lot of interest as a focus for study within the domain of Intrusion Detection Systems (IDS) (Hemraj et al., 2024) and plays an important role in network security monitoring. A variety of approaches, traditional and modern, have been used to detect anomalies in networks. Traditional signature-based detection has been proposed and used (Rahman et al., 2022). Signature-based detections analyze network data to detect threat signatures, enabling the recognition of known attacks. To flag an attack, signature-based detection relies on a database of known malicious patterns (Díaz-Verdejo et al., 2022). Traditional threat modeling approaches like Spoofing, Tampering, Repudiation, Information disclosure, Denial of service and Elevation of privilege (STRIDE) and Common Attack Pattern Enumeration and Classification (CAPEC) (Tariq et al., 2024) have been used in 5G networks to analyze vulnerabilities. However, these methods require prior information for anomalies to be detected, which is unsuitable against newly emerging or previously unseen patterns that may not yet have corresponding labels. This method relies on predefined attack patterns, limiting its effectiveness against unknown attacks (Deepika et al., 2024b) and may be unsuitable for 5G networks where patterns constantly change. Moreover, signature-based methods often struggle to identify attacks in their early stages, leaving networks vulnerable to prolonged disruptions and potential data breaches.

To overcome the shortcomings of the traditional signature-based technique, modern approaches have been proposed and used in anomaly detection. (Bouke & Abdullah, 2024) identified Machine Learning (ML) as a tool to introduce intelligence to network management. Learning can be supervised, semi-supervised and unsupervised learning-based (Saranya et al., 2020). Figure 1 below shows the taxonomy of ML.

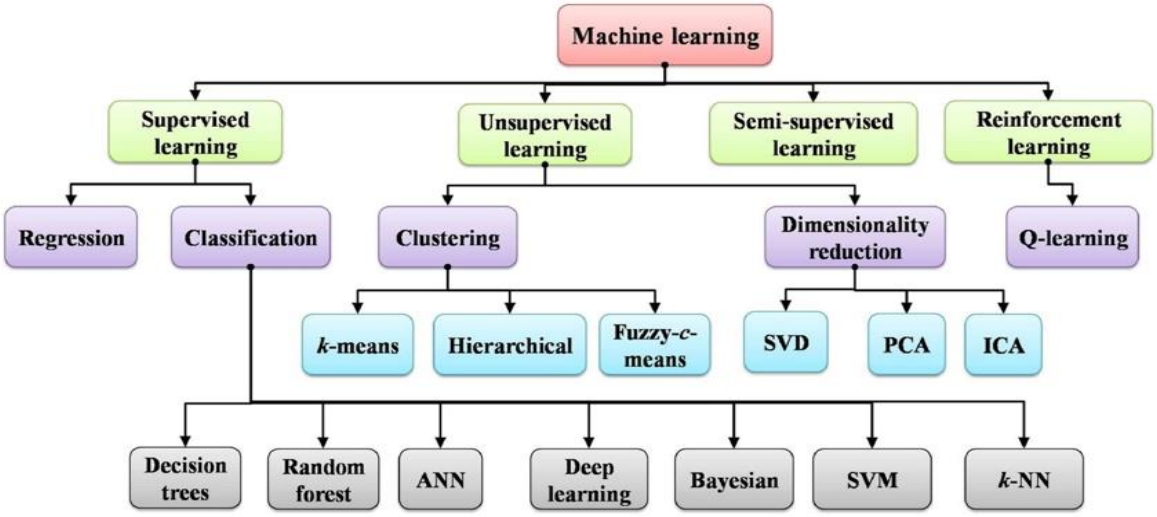

Figure 1: Taxonomy of Machine Learning

Supervised learning-based techniques utilize datasets that are labeled to train algorithms for precise data classification and outcome prediction (Sinha et al., 2024). In anomaly detection, supervised learned based models require that all data be clearly labeled as normal or abnormal. Several studies have examined the effectiveness of supervised learning-based algorithms in detecting anomalies in computer networks. (Hirsi et al., 2024) proposes an approach for traffic classification, identifying and detecting Distributed DDoS attacks within Software-Defined Networks (SDN) using Logistic Regression, Support Vector Machine (SVM), Random Forest, K-Nearest Neighbor, and XGBoost.

Similarly, (M et al., 2025) used random forest for identifying and classifying cyberattacks. Although useful for many tasks, Random Forest can be time-consuming and memory-intensive, especially for large trees and feature sets. (Ayush et al., 2024) conducts a comparative study of supervised models, Random Forest, XGBoost, and KNN for the 5G-NIDD dataset and for UNSW-NB 15, using Histogram-based Gradient Boosting to predict the benign or malicious attacks.

Unsupervised learning finds hidden structures in data that is not labeled (Sutton & Barto, 2018). It utilizes collections of unlabeled data for training. Some of the algorithms are k-means clustering and probabilistic clustering methods. Several studies have examined the effectiveness of supervised learning-based algorithms in detecting anomalies in computer networks.

(Deepika et al., 2024b) uses a combination of DBSCAN and Isolation Forest algorithms to detect anomalies in wireless network systems. This combination achieves high accuracy, precision, recall, F1 score and specificity with a low error rate. Despite supervised and unsupervised learning being a great tool to introduce intelligence to network management, they cannot learn from interactions with their environment.

Reinforcement Learning (RL) is learning what to do and how to map situations to actions to maximize a numerical reward signal (Malik & Singh Saini, 2023). The reinforcement learner is not told which actions to take. According to Sutton & Barto (2018), the agent has to exploit its prior experience and explore new actions to make better actions in the future. The agent interacts with their environment, utilizing past experiences to inform its decision. The agent learns to choose or avoid certain actions based on their consequences. To maximize reward, the learning agent must prioritize actions it has previously explored and proven effective in yielding positive outcomes.

Figure 2 below shows the interaction of an agent and the environment. The interaction occurs at time steps, t = 0, 1, 2, 3…, where information about the environment state St is received by the agent.

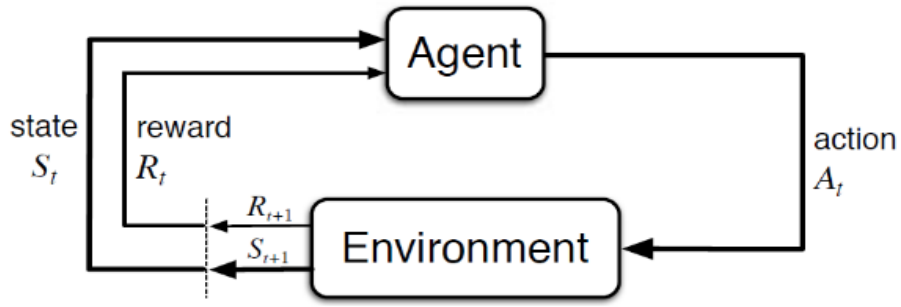

Figure 2: Interaction Between the Agent and the Environment

The agent decides an action At by referring to the state of the environment at point t. After that, the agent will get a signal that is a numerical reward Rt+1. This becomes a sequence (S0, A0, R1, S1, A1, R2…).

The state is an input used by the RL agent in policymaking. This means that the state should be as correct as possible.

RL-based techniques have been studied in network anomaly detection. (Ahmad et al., 2021) presents an innovative application of RL in Zero Trust Networks (ZTNs), identifying models that significantly improve network adaptability and performance against cyber threats. They highlight how RL models can adapt to evolving threats and complex environments, improving decision-making processes and reducing both false positives and negatives. Choi et al., (2023) and Amol et al,. (2024) present an Adaptive Intrusion Detection System (AIDS) that leverages RL-based Autoencoders to detect and respond to cyber intrusions in cyber-physical system environments. The proposed model proved effective in addressing the dynamic and complex nature of cyber-physical systems environments. Yun et al,. (2024) propose a deep reinforcement learning framework that utilizes partially labelled data to detect known and unknown anomaly patterns within large-scale time series data in manufacturing processes. The model demonstrated the ability to learn known anomaly patterns while effectively searching for potential anomalies in unlabeled data.

3. Theoretical Framework

3.1 Behaviorist Theory

Behaviorism, also known as the stimulus-response theory, proposed by (Catania & Laties, 1999), highlights the importance of rewards and punishment in shaping behavior. Scholars have applied behaviorist theory to emphasize learning as a process driven by interaction with the environment and the consequences of action. (Sutton & Barto, 2018) utilized these principles in their seminal work on reinforcement learning, where agents learn optimal actions through environmental interactions and feedback. Similarly, Mnih et al. (2015) applied behaviorist principles in their development of Deep Q-Networks (DQN), combining reinforcement signals with deep learning to enable agents to master tasks in playing Atari games. The main tenets of this theory include stimulus-response associations, the role of external feedback, and the idea that behavior can be conditioned through repeated exposure to positive or negative consequences.

3.2 Markov Decision Process Theory

Markov Decision Process (MDP) is a 4-tuple (S+, A, Pa, Ra) where S+ is a set of all possible states called the state space (Malik & Singh Saini, 2023). MDP theory was applied since RL often models decision-making in uncertain environments using MDPs. The MDP approach could frame how states (network conditions), actions (responses to potential anomalies), and rewards (detection accuracy) interact to optimize anomaly detection in the complex and dynamic 5G environment.

4. Methodology

This research, guided by a postpositivist worldview, employed a quantitative approach to investigate existing techniques used by Local Network Facility Providers in detecting anomalies in 5G networks. The quantitative approach allowed the use of quantitative data collection and analysis methods to gain knowledge (Friedl-Knirsch & Anthes, 2024). An experimental research design was used to design and validate a reinforcement-based machine learning model for anomaly detection in 5G and beyond networks. The study employed non-probabilistic sampling methods, as they allow for the use of nonrandom sampling methods, often relying on judgment and convenience rather than randomization (Giri, n.d.). Convenience sampling was used to select the Network Facility Provider in Tier 1, 2 and 3 based on their willingness to

participate. Network Facility Providers had stringent data privacy and security policies and sharing internal data, even for research purposes, can raise concerns about potential breaches, competitive disadvantages, and reputational risks. Purposive sampling was used to select study respondents within the local Network Facility Provider firms. This ensured that only individuals with relevant expertise in managing, monitoring and securing 5G network infrastructure were included. The target study respondents consisted of network management professionals from key technical departments, network operations center managers and related technical personnel who were directly involved in monitoring, managing, and securing 5G and beyond network infrastructure. Their expertise ensured that the collected data is relevant, reliable, and reflective of real-world operational challenges and strategies in ISP network management.
A questionnaire survey was administered to gather data from network professionals within a sample of 11 Network Facility Providers. The questionnaire helped to develop an understanding of the existing techniques used by local Network Facility Providers in detecting anomalies and also to assess the performance of these techniques. The questionnaire was organized into sections covering respondent background, anomaly detection tools in use, performance assessment, and perceived gaps in current systems. It was distributed online via Google Forms to ensure broad and safe accessibility, especially given the geographical and organizational dispersion of the respondents. Before deployment, the questionnaire was subjected to expert review for content validity and pilot-tested with a small group of network engineers to ensure clarity, reliability, identify unclear questions, and assess the accessibility of the online forms. The feedback from these processes informed minor revisions, ensuring that the instrument was aligned with the study objectives and capable of generating reliable and actionable data.

Experiment

A combination of software, libraries and hardware tools was utilized. The development environment was Google Colab. Colab was chosen for its flexibility and its pre-installed learning libraries, eliminating local setup complexities. On the software, the Python programming language was used to implement the model. Python is extensively used in machine learning because it has a wide range of modules and frameworks available. The core libraries used included PyTorch for building and training the DQN, NumPy for numerical operations, Pandas for dataset preprocessing and manipulation, and Scikit-learn for data splitting and evaluation metrics. Seaborn and Matplotlib were used for data visualization and pattern exploration. Hardware tools included a personal computer running on Windows 11 with an Intel Core i7 Processor, 16GB of RAM and a stable internet connection, which facilitated access to cloud-based resources. Google Colab cloud infrastructure provided NVIDIA TESLA T4 GPUs.

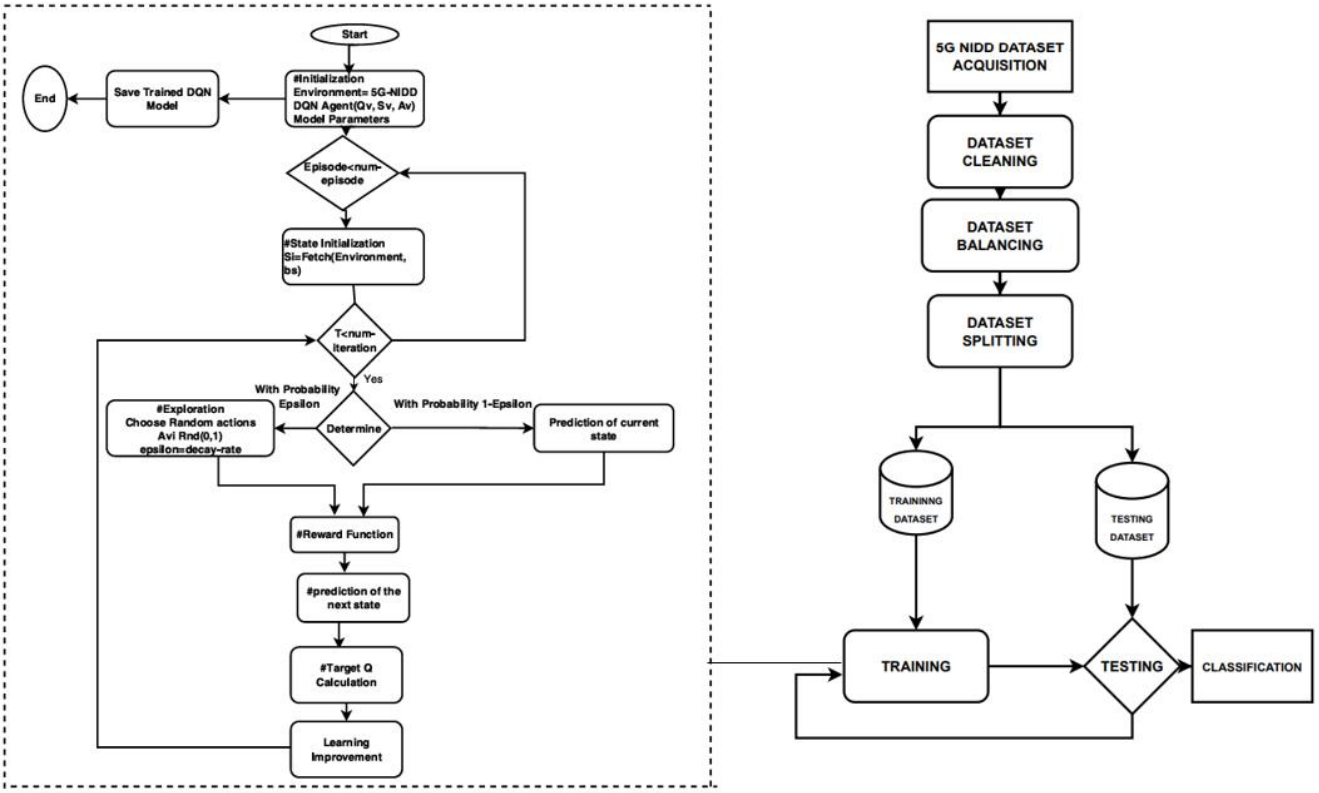

Figure 3: Overview of the Experiment Setup and Training Process

Dataset Acquisition

Most network service providers are reluctant to publicly share their 5G traffic data (Choi et al., 2023). As a result, the 5G-NIDD dataset was downloaded from Kaggle in CSV format and loaded into a Google Colab environment. The 5G-NIDD dataset comprises both normal traffic and malicious traffic data obtained from a 5G testbed situated within the 5G Test Network (5GTN) at the University of Oulu in Finland (Samarakoon et al., 2022). The dataset is generated from two distinct base stations, each of which includes both malicious attacker nodes and normal 5G users. The attacker nodes are responsible for launching eight types of attacks on the server within the 5GTN Multi-Access Edge Computing (MEC) setup. These attacks encompass DoS attacks and port scans. Specifically, the 5G-NIDD dataset includes the following instances, as shown in the table below

Table 2: 5G-NIDD Dataset Attack Types and Description

Attack Type	Description
Benign	Legitimate network traffic
UDPFlood	Flood UDP packets to exhaust resources
HTTPFlood	Send massive HTTP requests to the web server
SlowrateDoS	Slow requests to hold the connections
TCPConnectScan	Full TCP handshake scan for open ports
SYNScan	SYN packets only scan for ports
UDPScan	UDP packets scan for available services
SYNFlood	SYN handshake flood to exhaust the connection queue

ICMPFlood	Flood ICMP echo requests (ping)

Dataset Cleaning

Data preprocessing was performed to convert the 5G-NIDD data into a clean, consistent and suitable format for analysis. During the initial inspection of the dataset, the presence of null or missing values was revealed. Some columns were either dropped or filled with default values based on their relevance and completeness.

Dataset balancing

The dataset exhibited class imbalance, as shown in Figure 4 below, particularly with benign traffic dominating over specific attack types. The number of malicious traffic was smaller compared to benign traffic.

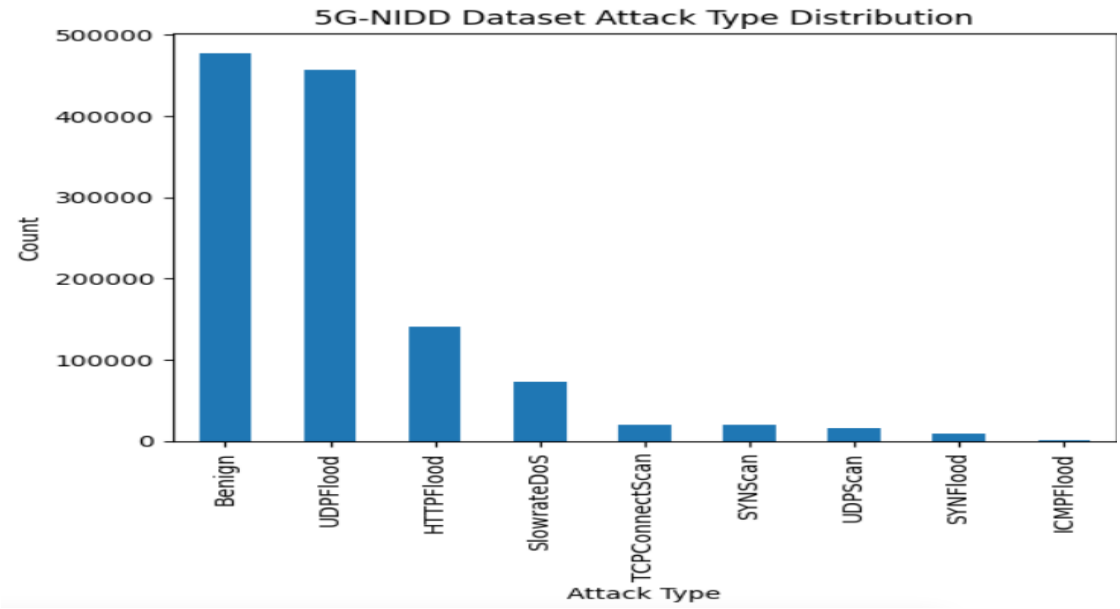

Figure 4: 5G-NIDD Dataset Attack Type Distribution

The dataset comprises 1,215,890 rows, with 39.29% representing benign traffic and 60.71% representing Malicious traffic, and 9 classes of attacks. To mitigate bias and improve generalization, under sampling and oversampling techniques were applied. Synthetic Minority Oversampling Technique (SMOTE) was used to generate instances of the minority class, enhancing the dataset balance. Under-sampling was applied to Benign, HTTPFlood, UDPFlood, and SlowrateDoS classes. Oversampling using SMOTE was applied to ICMPFlood, SYNFlood, SYN Scan, TCP Connect Scan, and UDP Scan.

Dataset Splitting

The dataset was partitioned into a training and test set using a 7:3 split ratio, where 70% of the data was used for training, whereas 30% for testing purposes. One attack class was intentionally removed from the training data. During testing, instances of that withheld class were included in the test set to simulate a new attack.

Model Training using Deep Q Learning

The Deep Q-Learning (DQL) model was trained using a reinforcement learning framework shown in

Figure 3 above. The training process began with the initialization of the environment, the agent, and model parameters.

The environment was constructed using the 5G-NIDD dataset with 46 input features, corresponding to traffic characteristics. The action space was defined by 9 discrete attack classes, representing both benign and malicious categories. Training was conducted over a fixed number of episodes, with each episode beginning by resetting the environment to an initial state. A state corresponded to the feature vector of a traffic instance. Within each episode, the agent interacted with the environment until termination. An epsilon greedy policy was applied to balance exploration and exploitation. At each step: With probability 1−ϵ1-\epsilon1−ϵ, the agent selected the action with the highest predicted Q-value. With probability epsilon, the agent selected a random action from the action space. The exploration rate epsilon decayed multiplicatively from 1.0 to a minimum of 0.1 with a decay factor of 0.98.

The RL agent's behavior was guided by a custom reward function designed to reflect the relative severity of misclassifications and to prioritize accurate detection of network anomalies. The function assigned different reward values based on whether the traffic was benign or malicious and whether the agent's classification was correct or incorrect. A replay buffer was implemented to store past experiences as tuples.

5. Results

5.1 Questionnaire Results

Twenty-nine participants were included in this research. All participants agreed to participate in the study after providing informed consent.

Regarding their current role within their respective network facility provider organizations, the majority of respondents occupied roles directly related to network operations, engineering, and security with 58.6% representing 17 participants were network engineers, 5 Network operations managers, and 3 security Architects. This suggests that the participants possessed relevant knowledge and practical experience in managing network anomalies and overseeing anomaly detection mechanisms within their organizations. 51.7% of the respondents were from Tier 3, 34.5% from Tier 2 and 13.8% Tier 1. The years of experience for the respondents are shown in Table 3 below.

Table 3: Distribution of Network Management Professionals by Years of Experience

Age	Frequency	Percentage
0	1	3.4
<2 Years	5	17.2
3-5 Years	16	55.2
6-10 Years	5	17.2
>10 years	2	6.9

The results revealed that all participants had at least some level of professional experience. A substantial proportion had more than 5 years of experience, indicating a knowledgeable respondent base. This reinforces the credibility of the feedback obtained, as it reflects insights from professionals with practical exposure to network operations and anomaly detection practices.

The respondents were asked to select the types of network anomalies most commonly detected in their operational environments. The results are summarized in Table 4 below.

Table 4: Commonly Detected Anomalies Distribution

Anomaly	Frequency	Percent
DOS	9	32.1
DDOS	11	39.3
Malware Infections	6	21.4
Unauthorized access	11	39.3
Network Congestion	17	60.7
Others	2	7.2

These findings underscore the real-world significance of this study's focus on automated detection of complex attack behaviors using reinforcement learning. The presence of DoS and DDoS attacks reported by respondents directly aligns with the attack types included in the 5G NIDD dataset used to train and evaluate the proposed model. This reinforces the dataset's representativeness and the practical relevance of the model's design. The presence of other anomaly types, such as unauthorized access and malware suggests that the threat landscape is diverse and evolving.

The respondents were asked to indicate the techniques and methods currently in use within their networks for anomaly detection. The results, summarized in Table 5 below, show that log analysis and traffic flow analysis were the most commonly used approaches, followed by log analysis and behavioral analysis.

Table 5: Anomaly Detection Method Distribution

Detection Technique/Method	Frequency	Percent
Log Analysis	16	57.1
Behavioral Analysis	11	39.3
Signature/Pattern Matching	7	25
Traffic flow analysis	21	72.4
Statistical Profiling	5	17.9
Network Congestion	17	60.7
Others	2	6.8

The prominence of log analysis and traffic flow analysis techniques indicates that many network operators rely on rule-driven or predefined pattern-matching systems for detecting known threats. While these methods are effective against well-documented attack vectors, they are typically limited in identifying adaptive attacks, or traffic anomalies that deviate from normal baselines. This observation strongly supports the motivation for this study to explore reinforcement learning as a more dynamic and adaptive approach to anomaly detection. Unlike static methods, reinforcement learning agents can learn from interaction with data environments, update their policies over time, and identify complex or evolving threats that may not match predefined signatures. The relatively low adoption of statistical anomaly scoring and behavioral analysis further suggests that advanced anomaly detection systems are not yet widespread, possibly due to implementation complexity, interpretability concerns, or resource constraints.

Respondents were asked to rate the effectiveness of their current anomaly detection techniques in identifying anomalies within 5G networks. As summarized in Table 6 below. The findings indicate that

the majority of respondents (53.6%) perceived their current anomaly detection techniques as "somewhat effective", suggesting that while these systems perform reasonably well, there remains significant room for improvement. This underscores the relevance of this research, as it aims to introduce a more adaptive, learning-driven approach through reinforcement learning.

Table 6: Responses to the Perceived Effectiveness of the Existing Anomaly Detection Techniques

Effectiveness	Count	Percent (%)
Very Ineffective	0	0
Somewhat Ineffective	1	3.6
Neutral	5	17.9
Somewhat Effective	15	53.6
Very Effective	7	25

Respondents were asked to identify the key challenges or pain points they experience with their current anomaly detection systems that are not adequately addressed by existing solutions. The responses captured through open-ended input revealed several recurring themes. A number of respondents expressed concern about the anomaly detection system's inability to detect modified attacks and poor adaptability to new attacks. Several responses highlighted that the lack of predictive analysis in the current systems raise alert after anomalies occur rather than anticipating them based on emerging behavior. This reactive nature limits operational foresight and fails to prevent service degradation before the impact. Many respondents emphasized that their current systems generate too many false positives, often due to a lack of contextual or domain-specific awareness. Factors such as user behavior patterns, time-based usage variations, or seasonal network activity are rarely considered. A number of respondents mentioned slow or delayed detection, particularly during peak traffic periods. This indicates that existing systems struggle to maintain performance under high-load 5G conditions, where network throughput and data flow fluctuate rapidly. These findings reveal that local internet facility providers face multi-dimensional challenges in managing anomaly detection in 5G networks.

Respondents were asked whether they are aware of reinforcement learning-based techniques being used for anomaly detection in network operations. 57.1% of respondents indicated that they had heard of reinforcement learning but had limited knowledge, 25% were aware and familiar with reinforcement learned based techniques. 17.9% of the respondents were not aware of the reinforcement learned based techniques used in anomaly detection.

Respondents were asked how likely their organization was to adopt reinforcement learned based techniques within their organizations. 53.6% of the respondents indicated that their organization was very likely to adopt reinforcement learning-based anomaly detection solutions within the next two years, with 25% somewhat unlikely and 10.7% somewhat unlikely. 10.7% indicated neutral.

5.2 Experimental Results

Training was conducted for 500 episodes. As shown in Figure 5, the learning process consistently improved with the increase in the number of episodes.

Figure 5: Graph of total rewards against episode

Early episodes recorded lower cumulative rewards, while later episodes showed steady improvement, reflecting enhanced policy learning and reduced misclassification. The accuracy of the model kept improving with the increase in the number of training episodes.

The model was first evaluated on attack types that were included in the training dataset. The reinforcement learning agent achieved consistently high detection performance. Accuracy, precision, recall, and F1-score values indicated that the model was able to classify known anomalies effectively, as shown in Table 6 below.

Table 7: Experimental Result Table

Anomaly Class	Precision	Recall	F1 Score
Benign	0.9651	0.6020	0.7415
HTTPFlood	0.6799	0.8117	0.7400
ICMPFlood	0.9670	1.000	0.9832
SYNFlood	0.8876	0.2826	0.4287
SYNScan	0.7514	0.5866	0.6588
SlowrateDos	0.5647	0.8514	0.6790
TCPConnectScan	0.7421	0.6446	0.6899
UDPFlood	0.7671	0.9955	0.8665
UDPScan	0.7296	0.9982	0.8430

To evaluate the generalization ability of the model, the SYNFlood attack class was deliberately removed during training and later introduced at the testing stage. The results showed that the model was able to detect the unseen attack, although with slightly lower performance metrics compared to known attacks. This confirms that the proposed approach is capable of adapting to new, previously unobserved anomalies.

6. Conclusion

The study confirms the potential of reinforcement learning to address the anomaly detection problem in 5G network traffic data. The model proved to be effective in differentiating between benign and malicious traffic in the 5G-NIDD dataset.

7. Challenges

One of the challenges encountered in this research was the computational intensity associated with training the Deep Q agent on high-dimensional data. The training required considerable computational resources and extended the training durations, which constrained the speed and flexibility of experimentation. Also, the exploration-exploitation trade-off difficulty as the Deep Q agent had to find a balance between trying new strategies and relying on strategies that were already proven to work. Achieving this balance in a dynamic and evolving environment was demanding.

8. Recommendation for future studies

Future studies should consider exploring real-time anomaly detection capabilities within the context of a local Network Facility Provider's 5G traffic. This would provide valuable insights into their practical applicability. Additionally, further studies could investigate the development of hybrid models that integrate RL with other machine learning techniques, such as deep learning. Such hybrid approaches may leverage the strengths of multiple paradigms, potentially enhancing the accuracy of anomaly detection across diverse network conditions.

9. References

1. Ahmad, Z., Shahid Khan, A., Wai Shiang, C., Abdullah, J., & Ahmad, F. (2021). Network intrusion detection system: A systematic study of machine learning and deep learning approaches. Transactions on Emerging Telecommunications Technologies, 32(1), e4150. https://doi.org/10.1002/ett.4150
2. Ahmadi, C., & Chen, J.-L. (2024). Survey on Reinforcement Learning Techniques for Enhancing Security and Efficiency in Zero Trust Networks. 2024 10th International Conference on Applied System Innovation (ICASI), 427–429. https://doi.org/10.1109/ICASI60819.2024.10547956
3. Alanazi, M. H. (2023). Machine Learning-based Secure 5G Network Slicing: A Systematic Literature Review. International Journal of Advanced Computer Science and Applications, 14(12). https://doi.org/10.14569/IJACSA.2023.0141239
4. Alsaedi, A., Moustafa, N., Tari, Z., Mahmood, A., & Anwar, A. (2020). TON_IoT Telemetry Dataset: A New Generation Dataset of IoT and IIoT for Data-Driven Intrusion Detection Systems. IEEE Access, 8, 165130–165150. https://doi.org/10.1109/ACCESS.2020.3022862
5. Andrade-Hoz, J., Wang, Q., & Alcaraz-Calero, J. M. (2024). Infrastructure-Wide and Intent-Based Networking Dataset for 5G-and-beyond AI-Driven Autonomous Networks. Sensors, 24(3), 783. https://doi.org/10.3390/s24030783
6. Bouke, M. A., & Abdullah, A. (2024). An empirical assessment of ML models for 5G network intrusion detection: A data leakage-free approach. E-Prime - Advances in Electrical Engineering, Electronics and Energy, 8, 100590. https://doi.org/10.1016/j.prime.2024.100590
7. Casas, P., Fiadino, P., & D'Alconzo, A. (n.d.). Machine-Learning-Based Approaches for Anomaly Detection and Classification in Cellular Networks.

8. Catania, A. C., & Laties, V. G. (1999). PAVLOV AND SKINNER: TWO LIVES IN SCIENCE (AN INTRODUCTION TO B. F. SKINNER'S "SOME RESPONSES TO THE STIMULUS 'PAVLOV'"). Journal of the Experimental Analysis of Behavior, 72(3), 455–461. https://doi.org/10.1901/jeab.1999.72-455
9. Choi, Y.-H., Kim, D., Ko, M., Cheon, K., Park, S., Kim, Y., & Yoon, H. (2023). ML-Based 5G Traffic Generation for Practical Simulations Using Open Datasets. IEEE Communications Magazine, 61(9), 130–136. https://doi.org/10.1109/MCOM.001.2200679
10. Community Network and Service Provider Licence.pdf. (n.d.).
11. Cyber Security Report Q4 APRIL JUNE 2023-2024.pdf. (n.d.).
12. Deepika, D., Pogiri, D., Pandravisham, L. R., Prudvi, Y. K., & Ramannagari, S. R. (2024a). Anomaly Network Traffic Detection of Wireless Network System. 2024 5th International Conference on Electronics and Sustainable Communication Systems (ICESC), 703–708. https://doi.org/10.1109/ICESC60852.2024.10689805
13. Deepika, D., Pogiri, D., Pandravisham, L. R., Prudvi, Y. K., & Ramannagari, S. R. (2024b). Anomaly Network Traffic Detection of Wireless Network System. 2024 5th International Conference on Electronics and Sustainable Communication Systems (ICESC), 703–708. https://doi.org/10.1109/ICESC60852.2024.10689805
14. Díaz-Verdejo, J., Muñoz-Calle, J., Estepa Alonso, A., Estepa Alonso, R., & Madinabeitia, G. (2022). On the Detection Capabilities of Signature-Based Intrusion Detection Systems in the Context of Web Attacks. Applied Sciences, 12(2), 852. https://doi.org/10.3390/app12020852
15. Disha, R. A., & Waheed, S. (2021). A Comparative study of machine learning models for Network Intrusion Detection System using UNSW-NB 15 dataset. 2021 International Conference on Electronics, Communications and Information Technology (ICECIT), 1–5. https://doi.org/10.1109/ICECIT54077.2021.9641471
16. Friedl-Knirsch, J., & Anthes, C. (2024). Mixed Methods Designs for User Studies in Cross Reality. 2024 IEEE International Symposium on Mixed and Augmented Reality Adjunct (ISMAR-Adjunct), 161–165. https://doi.org/10.1109/ISMAR-Adjunct64951.2024.00042
17. Ghafir, I., Svoboda, J., & Prenosil, V. (2015). Network Monitoring Approaches An Overview. Third International Conference on Advances in Computing, Communication and Information Technology-CCIT 2015, 118–123. https://doi.org/10.15224/978-1-63248-061-3-72
18. Giri, O. P. (n.d.). Choosing Sampling Techniques and Calculating Sample Size.
19. Goswami, H., & Choudhury, H. (2022). Security of IoT in 5G Cellular Networks: A Review of Current Status, Challenges and Future Directions. International Journal of Communication Networks and Information Security (IJCNIS), 13(2). https://doi.org/10.17762/ijcnis.v13i2.4955
20. Hemraj, Sonia, Ashish, Gupta, G., Rana, A., & Gupta, A. (2024). Demystifying Intrusion Detection Process using Machine Learning Techniques. 2024 11th International Conference on Computing for Sustainable Global Development (INDIACom), 629–633. https://doi.org/10.23919/INDIACom61295.2024.10499111
21. Hirsi, A., Audah, L., Salh, A., Alhartomi, M. A., & Ahmed, S. (2024). Detecting DDoS Threats Using Supervised Machine Learning for Traffic Classification in Software Defined Networking. IEEE Access, 12, 166675–166702. https://doi.org/10.1109/ACCESS.2024.3486034

22. Huang, X. (2023). Research on Computer Network Intrusion Detection Algorithm Based on Deep Learning. 2023 IEEE International Conference on Electrical, Automation and Computer Engineering (ICEACE), 1122–1125. https://doi.org/10.1109/ICEACE60673.2023.10442632
23. John W. Creswell-Research Design_ Qualitative, Quantitative, and Mixed Methods Approaches-SAGE Publications, Inc (2009).pdf. (n.d.).
24. Khraisat, A., & Alazab, A. (2021). A critical review of intrusion detection systems in the internet of things: Techniques, deployment strategy, validation strategy, attacks, public datasets and challenges. Cybersecurity, 4(1), 18. https://doi.org/10.1186/s42400-021-00077-7
25. Kumar, A., & Choi, B. J. (2022). Benchmarking Machine Learning based Detection of Cyber Attacks for Critical Infrastructure. 2022 International Conference on Information Networking (ICOIN), 24–29. https://doi.org/10.1109/ICOIN53446.2022.9687293
26. M, S., S, S., V, S., & T, S. (2025). Securing Wireless Sensor Networks from Intrusions Using Machine Learning-Based Detection and Response. 2025 International Conference on Multi-Agent Systems for Collaborative Intelligence (ICMSCI), 236–241. https://doi.org/10.1109/ICMSCI62561.2025.10894251
27. Malik, M., & Singh Saini, K. (2023). Network Intrusion Detection System using Reinforcement learning. 2023 4th International Conference for Emerging Technology (INCET), 1–4. https://doi.org/10.1109/INCET57972.2023.10170630
28. Matlack, A. K., Boots, B. C., & Richardson-Gool, T. S. (2024). The Impact of Internet Connectivity in Navigating Online Social Networks: A Cross-Country Analysis. SSRN Electronic Journal. https://doi.org/10.2139/ssrn.4913130
29. Rehman, F., Mushtaq, F., & Zaman, H. (2024). A Host-based Intrusion Detection: Using Signature-based and AI-driven Anomaly Detection for Enhanced Cybersecurity*. 2024 4th International Conference on Digital Futures and Transformative Technologies (ICoDT2), 1–7. https://doi.org/10.1109/ICoDT262145.2024.10740248
30. Samarakoon, S., Siriwardhana, Y., Porambage, P., Liyanage, M., Chang, S.-Y., Kim, J., Kim, J., & Ylianttila, M. (2022). 5G-NIDD: A Comprehensive Network Intrusion Detection Dataset Generated over 5G Wireless Network (Version 1). arXiv. https://doi.org/10.48550/ARXIV.2212.01298
31. Saranya, T., Sridevi, S., Deisy, C., Chung, T. D., & Khan, M. K. A. A. (2020). Performance Analysis of Machine Learning Algorithms in Intrusion Detection System: A Review. Procedia Computer Science, 171, 1251–1260. https://doi.org/10.1016/j.procs.2020.04.133
32. Sathwik, T., Vishruth Reddy, T. S., Gangavarapu, V. R., & Bhaskaran, S. (2024). Detecting DDoS Attacks in Software-Defined Networking through the Utilization of Supervised and Unsupervised Learning Techniques. 2024 15th International Conference on Computing Communication and Networking Technologies (ICCCNT), 1–6. https://doi.org/10.1109/ICCCNT61001.2024.10723853
33. Sector Statistics Report Q4 2022-2023.pdf. (n.d.).
34. Sinha, A., Agrawal, A., Roy, S., Uduthalapally, V., Das, D., Mahapatra, R., & Shetty, S. (2024). AnDet: ML-Based Anomaly Detection of UEs in a Multi-cell B5G Mobile Network for Improved QoS. 2024 International Conference on Computing, Networking and Communications (ICNC), 500–505. https://doi.org/10.1109/ICNC59896.2024.10556379
35. Sutton, R. S., & Barto, A. G. (2018). Reinforcement learning: An introduction (Second edition). The MIT Press.

36. Tariq, S., Rodríguez, E., Masip-Bruin, X., Trakadas, P., Jukan, A., & López, D. R. (2024). Strategy for Modeling Threats in 5G and B5G Networks. 2024 IEEE 24th International Symposium on Cluster, Cloud and Internet Computing Workshops (CCGridW), 18–25. https://doi.org/10.1109/CCGridW63211.2024.00008
37. Vibhute, A. D., Khan, M., Patil, C. H., Gaikwad, S. V., Mane, A. V., & Patel, K. K. (2024). Network anomaly detection and performance evaluation of Convolutional Neural