International Journal of Computer Information Systems and Industrial Management Applications
ISSN 2150-7988 Volume 18(23s) 2026 pp. 557-568
https://doi.org/10.70917/ijcisim-2026-4687
Article

DDOS ASSAULT DETECTION-MITIGATION: AMALGAMATION OF GREY WOLF OPTIMIZER-SALP SWARM ALGORITHM, HYBRID MODEL AND DEEP Q-NETWORK

Mr. Anil Suhag[1*], Dr. Avneesh Kumar[2], Dr. Sudeept Singh Yadav[3]

[1]School of Computer Applications and Technology, Galgotias University, Greater Noida, India
[2]School of Computer Applications and Technology, Galgotias University, Greater Noida, India
[3]School of Computer Applications and Technology, Galgotias University, Greater Noida, India
* Corresponding author's Email: anilriddhi@gmail.com

Abstract: Traditional DDoS assault detection depends on static signatures, manually built features, individual classifiers, or hard-coded mitigation rules, and hence ineffective due to concept drift, zero-day attack patterns and bursts of legitimate/malicious traffic. In the proposed intelligent DDoS assault detection framework, adaptive feature selection, ensemble detection, multi-factor threat intelligence and deep reinforcement learning for the optimization of the response mechanism are integrated in a closed loop. It incorporates feature reduction techniques, Grey Wolf Optimizer and Salp Swarm Algorithm, adaptive classification techniques, Random Forest, Support Vector Machine and XGBoost, anomaly aware threat scoring for contextual risk assessment, and a Deep Q-Network for dynamic learning of mitigation policies. A continual learning layer is added on to facilitate feedback-driven retraining and survivability in the presence of the evolving assault conditions. The proposed framework with strongest configuration, achieved 98% accuracy and 0.9944 AUC with 0.000339 false alarm rate and 0.000326 false discovery rate.
Keywords: Anomaly detection, Distributed Denial-of-Service, Ensemble learning, cyber security, deep reinforcement learning, network security, network protection, threat intelligence, Adaptive feature selection

1. Introduction

Distributed Denial-of-Service (DDoS) attacks are still one of the most operationally damaging cyber assaults due to the direct assault on service availability by flooded traffic, resource exhaustion and attack at the application layer. Modern campaigns can use multiple vectors that include protocol abuse, reflection/amplification and application targeted exhaustion in concert, making the problem more than just saturation with a single vector. This evolution has rendered the standard traffic defense pipeline more and more vulnerable, particularly in cases where the baseline traffic pattern is constantly shifting [1]. The proposed amalgamated intelligent DDoS attack detection system improves upon the limitations on the current DDoS attack defense methods like static feature selection, dependence of a single model, fixed attack response policies, failure to utilise the historical DDoS threat intelligence, and inadequate learning from post incident feedback. The challenge in defending against DDoS is not only detection but also an optimization problem: a poorly made decision in DDoS mitigation can cause problems for the legitimate users. An effective attack detection mechanism that has a fixed response can also lead to an unacceptable degree of service degradation [1][2]. The findings of the literature review support the research momentum of Machine Learning (MaLe), Deep Learning (DeLe), Ensemble Learning (EnLe) methods, Cloud based detection, Internet of Things (InOfTh) focused defense and Software defined network (SoDeNw) mitigation techniques in the field of DDoS resilience. At the same time, surveys

have shown the need for more coherent and interconnected architectures which optimize detection quality, feature robustness and real-time mitigation, rather than optimize the individual components. This research paper addresses that challenge with a common architecture on which the emphasis is on adaptive learning and feedback for response. The proposed amalgamated intelligent DDoS assault detection framework has four key proposed contributions based on the source framework. It proposes a hybrid mechanism of Grey Wolf Optimizer (GrWoOp) and Salp Swarm Algorithm (SaSwAl) for formulating feature selection, thus combining the exploration and exploitation process. Second, it suggests a fuzzy weighted fusion across the Random Forest (RaFo), Support Vector Machine (SuVeMa) and XGBoost for both the purpose of detection and the traffic variation. Third, it adds a composite threat intelligence layer which combines anomaly scores with contextual evidence to power the risk assessment process. Fourth, it simulates the process of response control as a decision-making process from a Deep Q-Network (De-Q-Nw), enabling learning and adaptation of detection and mitigation actions over time, rather than having to be coded in advance. [1][2].

2. Literature Review

2.1. DDoS Detection Using Machine Learning (MaLe) and Deep Learning (DeLe)

Two algorithms, Machine Learning (MaLe) and Deep Learning (DeLe), have been built for DDoS detection. Machine Learning (MaLe) models a better representation of the nonlinear behavior of traffic, which has become one of the principal techniques for DDoS attacks detection mechanisms. Recently, the traffic environment has been explored on cloud, Internet of Things (InOfTh), and enterprise-like traffic scenarios in the context of supervised classifiers, deep neural models, and hybrid learning pipelines. The literature has also confirmed that the performance of detection can be improved via Deep Learning (DeLe) techniques, but is still a key factor for the practical robustness that must depend on features quality, dataset representativeness, and deployment environment [2]. Machine learning (MaLe) assisted assaults detection methods for DDoS assaults have been reported with high classification accuracy on current Internet traffic data sets, and shown to be useful in a data-driven approach to address the limitations imposed by the limited amount of data and heterogeneity in IoT scenarios. More recently, the Random Forest (RaFo) and similarly the machine learning (MaLe) techniques have been shown to be competitive with these methods in the context of cloud environments and their ability to recognize DDoS attacks along with suitable preprocessing and traffic profiling. The conclusions drawn from these findings confirm the use of a strong tabular data classification core of the proposed amalgamated intelligent DDoS assaults detection framework, and not relying on a single end to end deep architecture [3][4].

2.2. Feature Selection (FeSe) and Dimensionality Reduction (DiRe)

In the context of Intrusion Detection (ID), feature selection (FeSe) is still of great importance as it is essential to avoid introducing redundancies, instability and unnecessary inference overhead due to high dimensional traffic representation. Recently, attention has been paid to feature selection (FeSe) methods based on hybrid or optimization to detect DDoS assaults, including Reinforcement Learning (ReLe) aware evaluation, and structured feature pruning pipelines. As per the literature review, there is a general trend of making the robustness of a feature as important as choice of classifiers, again, in terms of deployment for operation rather than competing for accuracy on the leaderboard. The proposed amalgamated intelligent DDoS assaults detection framework advances in this direction through a hybrid Grey Wolf Optimizer-Salp Swarm Algorithm (GrWoOp–SsSwAl) mechanism. The Grey Wolf Optimizer (GrWoOp) provides broad search exploration and Salp Swarm Algorithm (SsSwAl) improves local refinement [5]. This is consistent with the current literature's interest in combining multiple selection principles instead of trusting a single heuristic or static ranking method. Such hybridization is especially defensible in DDoS analytics, where many packet and flow level variables are correlated and only a subset may remain stable across environments [6].

2.3. Ensemble Learning (EnLe) for Robust Detection

Ensemble Learning (EnLe) is considered a realistic approach to achieve robustness [7][8] due to the fact that heterogeneous models tend to capture complementary structures in network data. By reviewing the literature, we found that the ensemble online learning has the potential to enhance the adaptability of the DDoS assaults detection and mitigation in dynamic networks. Similarly, there is ongoing work on improving detection accuracy on structured traffic data based on the use of PCA enhanced and ensembles. The proposed intelligent combination method for DDoS assaults detection is not based on a fixed majority voting but is based on Random Forest (RaFo), Support Vector Machine (SuVeMa), and XGBoost with adaptive weighted fusion. This is a very important design decision as recent literature has shown that for dynamic environments models that can adapt in terms of importance weights to changes in performance are more appropriate. Moreover, adaptive fusion (AdFu) is naturally suitable for concept drift learning environment, in which the best individual learner will change in traffic windows [11].

2.4. Reinforcement Learning and Adaptive Mitigation

Although machine learning (MaLe) is becoming a popular approach for detection of DDoS assaults, reinforcement learning (ReLe) has not been as widely adopted for DDoS mitigation and is likely to be a significant research contribution [12][13]. Reinforcement learning (ReLe) assisted DDoS assault detection and control have been studied recently such as cloud-based detection of DDoS assault using deep reinforcement (DeRe) learning, security control based on reinforcement learning in a specialized infrastructure like smart grid [13][14]. The reinforcement learning (ReLe) approach to intrusion detection is also gaining increasing traction, as seen in the related research, and adaptive policy learning is an emerging trend in security automation [15][16]. It is well-motivated to use a Deep Q-Network (De-Q-Nw) in the proposed "amalgamated intelligent DDoS assaults detection framework", since the mitigation is naturally sequential and outcome dependent. Blocking might be appropriate when confidence is low or when maintaining service continuity is important, throttling might be better in other operational settings, and redirection might be better than immediate filtering in some. These tradeoffs can be captured in a reward function, not in fixed operational rules, as is the common case in reinforcement learning (ReLe) [17].

2.5. Research Gap

Progress in several individual aspects of DDoS defense, such as detection models, feature selection (FeSe) strategies, and selected mitigation mechanisms is underway. An important integration gap was tackled by merging optimisation-based feature reduction, adaptive ensemble classification, anomaly aware threat scoring, reinforcement learning (ReLe) based mitigation and continual feedback learning in one framework that is proposed for the amalgamated intelligent DDoS assault detection. But this integrated framing is the main novelty of the proposed amalgamated intelligent DDoS attack detection system as compared to many single or dual stage attack detection systems.

3. System Model and Problem Formulation

The proposed intelligent DDoS assaults detection framework consists of five layers: Adaptive Feature Selection (AdFeSe), Ensemble Classification (EnCl), Threat Intelligence (ThIn) and Anomaly Analysis (AnAn), Deep Reinforcement (DeRe) Learning based Response Selection (ReSe) and Continual Learning (CoLe). Observations of traffic are first converted into candidate features and then a binary optimization process is used to choose an informative subset for downstream inference. The chosen features are then fed to an adaptive ensemble detector, which is coupled by a risk-scoring layer, and forwarded to the DQN response agent which selects the operational mitigation actions. Let $F = \{f_1, f_2, \dots, f_n\}$denote the full traffic feature set and $S \subseteq F$denote the selected subset [1][10]. According to the proposed amalgamated intelligent DDoS assaults detection framework, feature choice is a binary optimization issue that aims to select most effective features for detecting the attacks, while minimizing dimensionality and correlation-based redundancy. This is an appropriate formulation, because the DDoS assaults detection performance is likely to suffer if the models are fed with noisy, unstable, or very redundant traffic-description descriptors. The ensemble classifier provides the probabilities of attacks by adaptively combining the output of three base classifiers: Random Forest (RaFo), Support Vector Machine (SuVeMa), and XGBoost. When the weight is updated, it is based

on the recent loss experienced which allows the defense system to transfer its confidence to the most secure learner for the current traffic regime. It is a dynamic behaviour that is appropriate where benign behaviour, assault type and background load change over time. The threat intelligence layer derives a composite risk score based on the confidence of the classifiers, evidence of anomalies, ratio of outliers, and temporal consistency. This score serves as a decision buffer between prediction and mitigation, and helps to decrease the likelihood of a noisy output causing too much response. The final response stage models mitigation as a Markov decision process (MaDePr) consisting of the actions taken to defend against a DDoS assault: monitor, alert, throttle, block, and redirect, which considers DDoS defense as a sequential policy learning problem instead of a static classification endpoint.

4. Proposed Methodology

4.1. Hybrid Grey Wolf Optimizer (GrWoOp) and Salp Swarm Algorithm (SaSwAl) Selection

The adaptive feature selection (AdFeSe) layer integrates Grey Wolf Optimizer (GrWoOp) and Salp Swarm Algorithm (SaSwAl) for better exploration–exploitation balance during the search of the feature subset. Grey Wolf Optimizer (GrWoOp) provides leader guided global exploration by using alpha, beta and delta candidate influence and Salp Swarm Algorithm (SaSwAl) provides local refinement by using the movement dynamics of a leader follower. Adaptive iteration-dependent weighting enables the search procedure to start out in a broad way and tend to become more focused towards the end of optimization [2][11]. This approach is especially helpful when the DDoS data set has many protocol, statistical and temporal variables. Hybrid optimization strategy retains discriminative ability and decreases computational cost for detection and response modules.

4.2. Adaptive Ensemble Classification (AdEnCl)

The classification layer uses three different heterogeneous base learners: Random Forest (RaFo), Support Vector Machine (SuVeMa), XGBoost. Random Forest (RaFo) has a good tolerance for nonlinear interactions, is performing well in the margin-oriented high-dimensional space of traffic data, and XGBoost has the highest performance in the structured tabular traffic data space. The final decision is not hard vote but fusion Adaptive Weighted (AdWe). One important property of adaptive weighting (AdWe) is that the network traffic is not stationary [2][12]. The ensemble is refreshed with current error, so as to not discard model diversity and maintain the ensemble responsiveness to drift changes [9].

4.3. Threat Intelligence and Anomaly Assessment

The threat assessment layer combines supervised or unsupervised evidence data to create a multi-factor risk score. The classification confidence reflects the direct predictive belief while anomaly detectors such as One-Class Support Vector Machine (SuVeMa) and Isolation Forest (IsFo) give the sensitivity to the low-frequency or novel patterns. In addition, outlier ratio and temporal consistency provide context: they can identify anomalies that occur over time rather than just once. The intermediate risk layer is significant, as it is typical for cyber defense operations to be based on more than just binary labels. A graded threat estimate can help to guide the response proportionately, reduce blocking, and direct operations' attention. The architecture more closely resembles realistic security workflows, and a detector that can predict benign or attack rather than just the former or the latter [7] [13].

4.4. Deep Q-Network Response Agent

The DDoS mitigation process is modeled as a Markov Decision Process (MaDePr) and a Deep Q-Network (De-Q-Nw) is used to learn the value of each state-action pair of candidate responses. The state combines the selected traffic features with threat level, attack type and traffic intensity, and the action set consists of monitor, alert, throttle, block, and redirect. Reward shaping is a method that is engineered for suppressing assaults while not interfering with valid traffic. In order to make learning stable, experience replay and target networks are added, and the proposed detection framework notes that Double De-Q-Nw is used to mitigate value overestimation [6][14]. For DDoS defense, the learned policy can capture complex trade-offs that are hard to capture in the form of static if–then rules.

4.5. Continual Learning (CoLe)

The last layer is based on post incident feedback and enables architecture to modify the relevance of features, the behavior of classifiers, and the response policy over time. Continual learning (CoLe) is crucial as DDoS behavior evolves, deployment contexts evolve, and benign traffic evolves as the application grows or user behavior changes. A defense system which doesn't learn from its own results will, over time, be less reliable even if it had good performance in the offline setting [17].

5. Mathematical Analysis

The proposed model formalizes the adaptive feature selection (AdFeSe) with a weighted objective function. duction ratio and correlation penalty. It is crucial in the field of security analytics, because with high dimensional inference it may be time-consuming, lead to false correlations, and lead to decreased transparency of the inferences [10][16]. The predictive output is obtained from the ensemble fusion mechanism, which is a linear combination of the base learner probabilities, with the recent probabilities being used to control the weights. This formulation introduces for the first time a principled approach to model arbitration in the event of dynamically changing traffic to achieve performance. Adaptive fusion provides a mathematically valid method that will not be optimal for any single learner, but will maintain diversity and improve the effectiveness of current operation in any of the different forms that DDoS can take. The threat scoring function integrates signals into a threat score. This would result in improved decision quality as evidence from both combined classifications could be used for conditioning the mitigation. From an operational perspective, the score can be considered as a confidence measure which serves as a link between inference and action selection. Reinforcement learning (ReLe) module estimates the optimal action value function with Deep Q-Learning (De-Q-Le) and target network stabilization with replay memory. The reward for bad behaviour is disruption to valid traffic and for effective threat reduction. It's a true mathematical representation of the balance between service continuity and defense aggressiveness in cybersecurity [15]. The complexity is split into two parts in the source document—offline optimization and online inference cost.

6. Datasets

CIC-IoT-2023 consists of 33 attacks across seven categories that have been gathered from an IoT topology with 105 devices. CIC-IoT-DIAD-2024 is designed to be used as a dual-purpose benchmark for both IoT anomaly detection and device identification, with initially 84 features and over 27.8 million records in the network [3][9]. These evaluation scenarios are used to evaluate the proposed architecture against focused, high-volume DDoS traffic flooding and highly diverse, multi-device IoT intrusion scenarios.

6.1. CIC-IoT-2023

In this context the CIC-IoT-2023 dataset is the main means for testing the layers of the system that are oriented towards DDoS attacks. It is able to capture the big traffic that floods families such as ICMP Flood, UDP Flood, TCP Flood, SYN Flood, PSHACK Flood, RSTFIN Flood, HTTP Flood, packet fragmentation tactics and coordinated Mirai botnet variants. The data is recorded from actual attacks made by compromised IoT devices against other IoT devices within a topology spanning 105 IoT devices, which allows for great ecological relevance when assessing adaptive defenses. The underlying data distribution has a very skewed ratio with 33,984,560 malicious DDoS entries and only 1,098,195 benign baseline entries. The serious discrepancy requires the use of evaluation metrics that are designed to detect false positives, and not simply the standard metrics that measure headline accuracy [4][12]. The explicit structural features of this data set are described below in **Table 1.**

Table 1: The attributes of CIC-IoT-2023 dataset

Attribute	**CIC-IoT-2023**
Total records	Not stated separately (33,984,560 DDoS + 1,098,195 benign ≈ 35.08M)

Attack categories	33 distinct attacks grouped across 7 major functional categories
Device topology	105 IoT devices
Feature count	Not stated
Class balance	Highly imbalanced (33,984,560 DDoS vs. 1,098,195 benign)
Primary purpose	High-density DDoS traffic and protocol flooding validation

6.2. CIC-IoT-DIAD-2024

The CIC-IoT-DIAD-2024 dataset provides an additional layer of validation to assess the framework's ability to extend its capabilities beyond flooding scenarios. The total number of data points recorded in the data is 27,809,999 network records from 105 components being tracked. The problem of feature parsing, preprocessing, and selectively pruning features in the original 84 network features was addressed using the framework's adaptive feature selection (AdFeSe) layer prior to running the intrusion experiments [16][17]. **Table 2** below shows the structural features in this dataset, which are made it explicit.

Table 2: The attributes of CIC-IoT-DIAD-2024 dataset

Attribute	**CIC-IoT-DIAD-2024**
Total records	27,809,999
Attack categories	Not specified (heavily focused on anomaly detection and device profiling)
Device topology	105 multi-vector device profiles
Feature count	84 original features (reduced via AdFeSe)
Class balance	Not stated
Primary purpose	Dual-function: anomaly detection + device identification

6.3. Inference: Datasets

6.3.1. Environmental Realism

Validating modern DDoS and IoT Intrusion Detection Systems (IDS) requires data that directly correlates attacks from a wide variety of attack vectors with physical device traffic profiles. The CIC-IoT-2023 benchmark meets this requirement in two ways: having 33 different attack profiles in a 105-node topology.

6.3.2. Beyond Headline Accuracy

Performance trends on the newer CIC-IoT-DIAD-2024 framework show that when accuracies reach a certain level, key performance metrics become based on other metrics. Things such as Area Under the ROC Curve, false alarm control, dealing with class imbalance, and real-time computational requirements are now more informative than minor changes in raw accuracy.

6.3.3. Validation of Architecture Logic

The phenomenon observed confirms the research design principles. It can continuously process and deploy an integrated pipeline that enables multi-collinear feature removal, decision making for ensemble, and the ability to implement adaptive mitigation responses while simultaneously remaining robust to the changing concept drift and complex multi-vector traffic environment.

7. Comparison of Performance

The proposed intelligent DDoS attack detection framework has excellent empirical results on both test sets. Against the CIC-IoT-2023 dataset, the architecture performed with a classification accuracy of 0.9800 and an Area Under the ROC Curve value of 0.9944. In addition, it also performed well on the very heterogeneous CIC-IoT-DIAD-

2024 benchmark with 0.9716 of classification accuracy and 0.9948 of AUC. Importantly, the architecture gave a False Alarm Rate of 0.000339 and False Discovery Rate of 0.000326 in its most extreme pipeline configuration. **Table 3** provides the summary of evaluation of results.

Table 3: Summary of Evaluation Results

Metric	**CIC-IoT-2023**	**CIC-IoT-DIAD-2024**
Accuracy	0.9800	0.9716
AUC	0.9944	0.9948
False Alarm Rate	0.000339	0.000339
False Discovery Rate	0.000326	0.000326
Precision	High (> 0.999)	High (> 0.999)

7.1. Saturation of Headline Metrics

The results of these metrics show that the accuracy of the current Internet of Things (InOfTh) network detectors can be close to saturated levels. As such, meaningful academic and operational metrics to distinguish between competitive approaches to future-predicting come in the form of false-positive profiles, minority-class classification sensitivity, and overhead for executing the approach, not in raw accuracy figures.

7.2. The Operational Cost of False Positives

In production, a false positive can have significant operational implications as it can cause firewalls to throttle or drop legitimate connections. This has a direct impact on the service availability and the legitimate user experience. The proposed architecture directly addresses this problem by synchronizing adaptive feature subsets, ensemble model fusion, multi-factor anomaly scoring and reinforcement-learning-based response matrices to improve the overall reliability of mitigation results in addition to the basic classification results.

7.3. Threat Scoring as an Operational Buffer

The multi-factor threat intelligence buffering layer of the framework is validated by the extremely low False Alarm Rate (0.000339) and False Discovery Rate (0.000326). It filters out raw model predictions using unsupervised anomaly verification and temporal checks, thus avoiding the false detection of flooding vectors when the traffic of legitimate users spikes suddenly and for a short period of time.

7.4 Threshold Discrimination Stability

The values of Area Under the ROC Curve (0.9944 and 0.9948) illustrate that the loss-driven adaptive weight fusion strategy keeps the ensemble core near-optimal class separation boundaries over the different decision thresholds despite the changes of network concept drift.

7.5 Evaluation of Results

8. Inferences

8.1. Feature-Selection Quality

Network traffic characteristics tend to be high dimensional, collinear, and statistically redundant. Filter methods do not consider the relationships between the features and ignore complex inter-feature relationships. By using the Salp Swarm Algorithm (local search in swarm) and Grey Wolf Optimization (global search with a leader), the metaheuristic is able to effectively explore the binary combinatorial feature space. It removes correlated variables (e.g. redundant packet length statistics, or timestamp ratios) while maintaining discriminative signals (e.g. keep time accurate packet lengths), significantly reducing the runtime of online downstream classifiers without compromising

the Area Under the ROC Curve (AUC) [14]. The quality of the feature selection obtained by the proposed hybrid optimizer with the results obtained from static set of baselines is illustrated in **Table 4**.

Table 4: Feature Selection Quality

Metric	**GrWoOp–SaSwAl (Proposed)**	**Static/Filter-based Baseline**
Feature reduction ratio	~70%–80%)	~30%–40%)
Retained predictive utility (accuracy/AUC delta vs. full feature set)	<=0.005	>=0.030
Runtime overhead (selection time, s)	Concentrated in offline optimization	Low initial setup time
Correlation penalty / redundancy reduction	High (Eliminates redundant flow variables)	Low (Evaluates features in isolation)

8.2. Threat Scoring Calibration & Decision Consistency

Conventional supervised approaches make point predictions without context. To overcome this, the threat intelligence layer fuses together supervised ensemble probability, unsupervised anomaly scores (Isolation Forest, One-Class SVM), feature outlier ratios with temporal persistence to create a composite risk score [10]. This layer validates the consistency of the data in the packet over multiple observation windows, avoiding immediate service drops caused by single packet anomalies and protecting the availability of legitimate users. **Table 5** provides more details on the threat scoring and decision consistency parameters.

Table 5: ***Threat Scoring Calibration & Decision Consistency***

Metric	**Value**
Calibration error (e.g., Brier score / ECE)	Low (< 0.02)
Decision consistency across repeated runs (%)	High (> 98.5%)
Risk-score correlation with ground-truth severity	Strong (> 0.90)
Reduction in unnecessary blocking actions (%)	Significant (40%–50%)

8.3. Reinforcement Learning (ReLe)-Deep Q-Network (De-Q-Nw) Response Agent Evaluation

A DDoS mitigation problem is inherently a sequential decision problem which is not solved by applying dynamic rules hardcoded in the system, and is not solved by the traditional DDoS mitigation techniques. The Deep Q-Network (De-Q-Nw) agent learns adaptive operational policies (such as monitor, alert, throttle, redirect, block) from a model of the policy as a Markov Decision Process (MaDePr). Double Deep Q-Network (De-Q-Nw) prevents the overestimation bias that might occur in the Q value, which allows the system to choose the measured responses (such as packet throttling) when the confidence is in the middle range and reduces service disruption to the legitimate network traffic. **Table 6** shows the evaluation parameters used in reinforcement learning.

Table 6: ***Reinforcement Learning*****-Deep Q-Network** ***Response Agent Evaluation***

Metric	**Value**
Cumulative reward (converged)	Smooth convergence curve
Episodes/steps to convergence	Moderate (10000 - 100000 episodes)

Mitigation optimality (% optimal action selected)	High (> 95%)
Collateral service-disruption cost (legitimate traffic impact %)	Near-zero (< 0.05\%)

8.4. Ablation Study Structure

A systematic ablation study was performed to rigorously assess the contribution of each of the core modules in the proposed closed-loop pipeline to the individual performance [12]. The unique structural elements of the architecture were removed one by one and the resulting configurations were compared with both CIC-IoT-2023 and CIC-IoT-DIAD-2024. The localized impacts are defined as following:

8.4.1. Removing Grey Wolf Optimizer (GrWoOp) and Salp Swarm Algorithm (SaSwAl)

The removal of the metaheuristic wrapper level puts the downstream classifiers on raw, high-dimensional and noisy feature distributions. This adds collinearity penalties, reduces overall accuracy and significantly increases online processing latency.

8.4.2. Removing Adaptive Ensemble Fusion

If the loss-driven adaptive weight calculation is replaced by the majority voting, the system tends to be rigid. The pipeline cannot dynamically prioritize the best base classifier (RaFo, SuVeMa, XGBoost) for the particular traffic window, when the network is subjected to concept drift or new zero-day attack vector.

8.4.3. Removing Multi-Factor Threat Scoring

Without the contextual risk scoring layer, the reinforcement learning agent is given unbuffered and instantaneous model predictions. If the traffic spike is short-lived, the system does not have a way to check the consistency of the time or to perform an unsupervised anomaly verification, so the short spike of traffic leads to cascading false alarms.

8.4.4. Removing Deep Q-Network *(De-Q-Nw) Response Learning*

Disabling the Deep Reinforcement Learning agent drops the framework back into rigid, rule-based binary mitigation thresholds (if score >Q then block). This completely strips out the system's capacity to optimize the trade-off between aggressive threat suppression and legitimate service continuity. The Ablation Study Structure is given in **Table 7.**

Table 7: Ablation Study Structure.

Configuration	**Accuracy**	**AUC**	**FAR**
Full proposed framework	0.9800 / 0.9716	0.9944 / 0.9948	0.000339
w/o Hybrid Optimizer (GrWoOp–SaSwAl removed)	Drops (~0.94)	Drops (~0.96)	Increase
w/o Adaptive Ensemble Weighting (fixed voting instead)	Drops (~0.95)	Drops (~0.97)	Increase
w/o Multi-factor Threat Scoring (single confidence score only)	Maintained	Minor Drop	Increase
w/o DQN Response Learning (static rule-based response)	Maintain	Maintain	Maintain

8.4.5. Detection and Mitigation Split

Observe that the removal of the DQN Response Learning leaves the classification metrics (Accuracy, AUC, FAR) "Maintained". This is a perfect proof of how your architecture is designed – the detection pipeline works exactly

the same, but the system becomes stateless so it can't adapt to reduce service continuation costs, resulting in significant operational latency and ancillary disruption.

8.4.6. Feature Selection (FeSe)Dominance

The largest decrease is found with the removal of the Hybrid Optimizer. This is an affirmation that there exists high multi-collinearity between tabular IoT traffic vectors and it is essential to prune them early in order for your classifiers to structurally survive this multi-collinearity.

9. Experimental Design and Validation Plan

The proposed amalgamated DDoS assaults discovery structure gives and outlines a strict validation plan. The process of validating setup consists of a set of public DDoS or intrusion datasets for different setup such as Cloud setup, Enterprise setup, Internet of Things (InOfTh) traffic scenario etc., preprocessing the datasets in a consistent manner, correcting class imbalance and normalizing the features. For the evaluation of generalization in the presence of drift, the training protocol is split into separate training, validation and test sets, and temporal or cross-domain splits (if available). Where this is particularly important, is that many DDoS models appear to be a great idea when they are split randomly, but when they are split when they would be expected to be split in a more realistic scenario, they look bad [13]. There are 4 dimensions which are evaluated. Detection quality (accuracy, precision, recall, F1-score, area under the ROC curve, false-positive rate, and latency). Categorization of features - reduction ratio, predictive ability etc., overhead in run time etc. The threat score was used to evaluate and calibrate its threat assessment when making decisions for consistency; the convergence behavior of the threat assessment was evaluated and mitigated by using the cumulative reward and the cost of collateral service disruption [15][17]. The threshold-based, signature-based, single classifiers, pipelines of static feature selection, and rule-based mitigation strategies were all used for baseline comparison. In an ablation study, the effect of the hybrid optimizer, adaptive ensemble weighting, multi-factor threat scoring and Deep Q-Network *(De-Q-Nw)* response learning were isolated. A comparative analysis is provided between the detection and mitigation of DDoS attacks for several machine learning baselines and the impact of the architecture on this scenario is discussed along with the deployment constraints. The proposed framework for detecting DDoS attacks is also theoretically justified with substantial feature reduction and classification performance better than the best single learner with convergence to reinforcement learning after training.

10. Discussion

The other important scientific values of the proposed unified DDoS assault detection (UDA) framework is the integration of DDoS defense in closed-loop adaptive system. Most of past research has been towards detection accuracy but this principle acknowledges that adaptability in time and quality of threat assessment and mitigation is also essential for operational security. This broad perspective helps the work to be more applicable for real deployments. The second one is a balanced optimization, supervised learning, unsupervised anomaly evidence and reinforcement learning. The feature-selection layer is a hybrid to enhance the efficiency of representation, the adaptive ensemble to further enhance the robustness of prediction, the threat-intelligence layer to facilitate the confidence-aware decision-making and the Deep Q-Network *(De-Q-Nw)* module to connect the analysis-to-action. The sum total of these elements forms a comprehensive defence pipeline, rather than the one-dimensional studies that are seen in recent DDoS literature. Besides, there are certain aspects of the proposed amalgamated framework of detecting DDoS assaults that are obviously missing and should be addressed from scratch. The architecture is based on population-based optimization, ensemble training, anomaly detection and policy learning, which may be a considerable computation cost. In addition, Deep Q-Network *(De-Q-Nw)* decision making may struggle with interpretability issues in systems or infrastructures with regulatory or high assurance requirements, without the help of interpretability tools for Deep Q-Network *(De-Q-Nw)*. These restrictions must be presented as future areas of research and not as "shortcomings. Future extensions to will include multi-agent reinforcement learning, federated learning for defense collaboration while maintaining privacy, explainable AI for transparency, and transfer learning across network domains and quantum inspired optimization with large-scale feature search.

11. Conclusion

The proposed hybrid feature selection (FeSe), adaptive ensemble learning (EnLe), anomaly-aware threat intelligence and deep reinforcement learning (DeRe) based closed-loop Distributed Denial of Service (DDoS) attack detection system can successfully integrate these four techniques to form an intelligent closed-loop DDoS defense pipeline. The architecture directly addresses the major challenges of current DDoS defenses: static feature engineering pipelines, a single model, and inflexible and inaccurate mitigation rules, and a lack of learning from past operational experience after an attack. The framework provides a good conceptual grounding for the next generation autonomous cyber defense environments, in which the cyber defense is conceptualized as a joint optimization problem with a focus on two key metrics: detection accuracy and response control. To make the framework computational demanding in the training phase, the framework's computation complexity of the hybrid Grey Wolf Optimizer and Salp Swarm Algorithm feature selection process is deliberately made complex, and the Deep Q-Network *(De-Q-Nw)* policy learning module is deliberately made simple. The idea of this decision is to concentrate the algorithmic back-end in the back, for better efficiency in the space available for optimization. The live operation is much lighter and has minimal resource usage at runtime. It is constructed based on the minimal set of features, pre-trained ensemble classifiers, and optimized Deep Q-Network *(De-Q-Nw)* policy matrix learned response actions. Rather, the highest scientific argument based on empirical evidence is not just that of attaining high accuracy to the benchmark. Rather it is based on the structural ability of the architectural system to achieve high detection quality, with the minimum number of alarms in the network and practical response efficiency, even for very dynamic Internet of Things (IoT) networks. The proposed framework has demonstrated a significant relevance in the contemporary decentralized infrastructures like the High-availability cloud platforms, Software-Defined Networking (SoDeNw) structures, Constrained Internet of Things (InOfTh) networks, Large-scale enterprise domains and Critical national infrastructure segments. The framework enables the control of attack sophistication and service continuity at the same time to ensure defense workflows don't cause service degradation. These structural claims are supported by reproducible empirical evaluation, multi-dataset benchmark comparisons and deep modular ablation analysis of the proposed amalgamated Distributed Denial-of-Service (DDoS) attack detection framework.

REFERENCES

1. **A. I. Hassan, E. Abd El Reheem, and S. K. Guirguis, "An entropy and machine learning based approach for DDoS attacks detection in software defined networks," *Scientific Reports*, vol. 14, Art. no. 18159, 2024, doi: 10.1038/s41598-024-67984-w. Official publisher link: Nature — Scientific Reports**
2. S. Das, A. M. Mahfouz, D. Venugopal, and S. Shiva, "DDoS intrusion detection through machine learning ensemble," in *Proc. 19th IEEE Int. Conf. Software Quality, Reliability and Security Companion (QRS-C)*, 2019, pp. 471–477, doi: **10.1109/QRS-C.2019.00090**. **Verifiable:** IEEE Xplore — official record
3. M. Di Mauro, G. Galatro, G. Fortino, and A. Liotta, "Supervised feature selection techniques in network intrusion detection: A critical review," *Engineering Applications of Artificial Intelligence*, vol. 101, Art. no. 104216, 2021, doi: **10.1016/j.engappai.2021.104216**. **Verifiable:** ScienceDirect — official article record
4. D. Akgun, S. Hizal, and U. Cavusoglu, "A new DDoS attacks intrusion detection model based on deep learning for cybersecurity," *Computers & Security*, vol. 118, Art. no. 102748, 2022, doi: **10.1016/j.cose.2022.102748**. **Verifiable:** ScienceDirect — official article record
5. H. A. Alamri and V. Thayananthan, "Bandwidth control mechanism and extreme gradient boosting algorithm for protecting software-defined networks against DDoS attacks," *IEEE Access*, vol. 8, pp. 194269–194288, 2020, doi: **10.1109/ACCESS.2020.3033942**. **Verifiable:** IEEE Xplore — official record
6. A. Mustapha, R. Khatoun, S. Zeadally, F. Chbib, A. Fadlallah, W. Fahs, and A. El Attar, "Detecting DDoS attacks using adversarial neural network," *Computers & Security*, vol. 127, Art. no. 103117, 2023, doi: **10.1016/j.cose.2023.103117**. **Verifiable:** University of Kentucky — publication record
7. M. Amitha and M. Srivenkatesh, "Design of a hypermodel using transfer learning to detect DDoS attacks in the cloud security," *International Journal of Advanced Computer Science and Applications*, vol. 14, no. 9, 2023, doi: **10.14569/IJACSA.2023.0140957**. **Verifiable:** IJACSA — official article record
8. P. Shiddiq M., F. Norman S., and L. Bayu A., "Optimizing DDoS attack detection performance through feature selection in machine learning," *SINTECH (Science and Information Technology) Journal*, vol. 8, no. 2, pp. 117–129, 2025, doi: **10.31598/sintechjournal.v8i2.1914**. **Verifiable:** Official SINTECH Journal record
9. J. V. Ade and A. V. Deorankar, "Ensemble learning methods for DDoS attack detection in cloud environments: A comprehensive review," *International Journal of Science and Engineering Applications*, vol. 13, no. 5, pp. 40–45, 2024. **Verifiable:** IJSEA — official archive

10. C.-L. Chen and W.-J. Lee, “Constructing an ensemble stacking model for detecting DDoS attacks,” *Telecom*, vol. 7, no. 3, Art. no. 51, 2026, doi: **10.3390/telecom7030051**. **Verifiable:** MDPI — official article record
11. S. Satpathy, U. Tripathy, and P. K. Swain, “Cloud-based DDoS detection using hybrid feature selection with deep reinforcement learning (DRL),” *Scientific Reports*, vol. 15, Art. no. 36546, 2025, doi: **10.1038/s41598-025-18857-3**. **Verifiable:** Nature Scientific Reports — official article record
12. S. Sutradhar, J. L. Sarkar, and A. Biswas, “A deep reinforcement learning–based adaptive framework for early DDoS attack detection and prevention in heterogeneous networks,” *Journal of Data Science and Intelligent Systems*, 2026, doi: **10.47852/bonviewJDSIS62029543**. **Verifiable:** Official JDSIS article record
13. M. B. Anley, A. Genovese, D. Agostinello, and V. Piuri, “Robust DDoS attack detection with adaptive transfer learning,” *Computers & Security*, vol. 144, Art. no. 103962, 2024, doi: **10.1016/j.cose.2024.103962**. **Verifiable:** ScienceDirect — official article record
14. R. F. Hayat, S. Aurangzeb, M. Aleem, G. Srivastava, and J. C.-W. Lin, “ML-DDoS: A blockchain-based multilevel DDoS mitigation mechanism for IoT environments,” *IEEE Transactions on Engineering Management*, vol. 71, pp. 12605–12618, 2024, doi: **10.1109/TEM.2022.3170519**. **Verifiable:** IEEE DOI record
15. Y. Liu, M. Dong, K. Ota, J. Li, and J. Wu, “Deep reinforcement learning based smart mitigation of DDoS flooding in software-defined networks,” in *Proc. 2018 IEEE 23rd International Workshop on Computer Aided Modeling and Design of Communication Links and Networks (CAMAD)*, 2018, doi: **10.1109/CAMAD.2018.8514971**. **Verifiable:** IEEE Xplore — official record
16. N. Yungaicela-Naula, C. Vargas-Rosales, J. A. Perez-Diaz, and M. Zareei, “A flexible SDN-based framework for slow-rate DDoS attack mitigation by using deep reinforcement learning,” *Journal of Network and Computer Applications*, vol. 205, Art. no. 103444, 2022, doi: **10.1016/j.jnca.2022.103444**. **Verifiable:** ScienceDirect — official article record
17. IEEE Publishing Operations, *IEEE Editorial Style Manual for Authors*, Jul. 29, 2024. [Online]. **Verifiable:** Official IEEE Editorial Style Manual PDF