International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 06 , June - 2026

FeDrift: Feature-Level Drift Evolution Analysis for Adaptive DDoS Detection in Dynamic Networks

Amrendra Kumar Sharma*
Department of Computer Application
Chhatrapati Shahu Ji Maharaj University, Kanpur, India
ORCID iD: https://orcid.org/0009-0000-5616-5179
*Corresponding Author

Mamta Tiwari
Department of Computer Application
Chhatrapati Shahu Ji Maharaj University, Kanpur, India
ORCID iD: https://orcid.org/0000-0002-5217-4841

Abstract: The dynamic nature of modern network environments presents significant challenges to intrusion detection systems, as evolving traffic patterns can lead to concept drift and degrade detection performance over time. Conventional machine learning-based intrusion detection approaches generally assume static data distributions and often fail to adapt effectively to changing network behaviors. To address this limitation, this paper proposes FeDrift, an adaptive drift-aware framework for distributed denial-of-service (DDoS) attack detection in evolving network environments. The proposed framework integrates feature-level drift quantification using the Wasserstein distance, adaptive threshold-based drift detection, selective model adaptation and incremental learning within a unified detection architecture. Network traffic is processed as a continuous stream and analyzed through consecutive temporal windows to capture evolving feature distributions and identify significant concept drift events. The effectiveness of the proposed approach is evaluated using the CICIDS2017 and four incremental learning classifiers, namely Stochastic Gradient Descent, Passive Aggressive, Gaussian Naïve Bayes and Perceptron. Experimental results demonstrate that the proposed adaptive mechanism successfully identifies significant drift events while reducing unnecessary model adaptations. Compared with a fixed-threshold strategy, FeDrift reduced drift-triggered adaptations by 93.33%, detecting only two significant drift events throughout the traffic stream. Furthermore, the PA classifier achieved the highest detection accuracy of 99.71%, while maintaining stable performance under evolving traffic conditions.

Keywords: Intrusion Detection System, Concept Drift, DDoS Detection, Incremental Learning, Adaptive Thresholding, Feature Drift Analysis

1. INTRODUCTION

Cloud computing, IoT, and large-scale networked systems are becoming more prevalent and this has further exacerbated the Distributed Denial of Service (DDoS) attack risk. An intrusion detection system (IDS) for detecting malicious traffic has been developed to perform well in the detection of malicious traffic but the dynamic network environment often results in poor performance after deployment [1]. The distributions of the data underlying the models change as the manner in which they are used, how many users are using them, how they are configured, and how attacks are carried out, change on a regular basis, making the models less reliable over time [2]. This problem is known as concept drift, which is the case in which the statistical characteristics of the data changes and thus the training environment is different from the operational environment [2][3].

Concept drift represents one of the primary challenges in deploying machine learning-based IDS in operational environments. It often occurs in conjunction with feature drift where features or the importance and frequency of their presence in the network change while attack behavior changes [1]. This can cause a substantial loss of accuracy in detections, false alarms and diminished AI security system robustness [4]. In cybersecurity applications, this challenge is particularly critical because attack behaviors evolve continuously and novel attack variants frequently emerge. Consequently, IDS models that perform well during offline evaluation often experience substantial degradation when deployed in long-term streaming environments [5].

Several drift detection methods have been suggested to detect the change in distribution for streaming data [3]. Traditional methods evaluate either the performance of the classifiers or their statistical deviations while recent unsupervised methods consider statistical changes directly on data distributions without any labeled instance [2]. Moreover, adaptive cybersecurity frameworks have shown the significance of combining drift detection and model adaptation to keep the detection performance stable over time in the presence of changing threats [1]. Despite such developments, the current methods are mainly based on detecting drift rather than on understanding the changes undergone by individual network features. Also, these methods rely primarily on classifier performance degradation, prediction errors or ensemble disagreement as indicators of drift. Moreover, overly sensitive drift detectors frequently trigger excessive retraining events, increasing computational overhead and reducing deployment efficiency in resource-constrained environments [6][7].

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 06 , June - 2026

In DDoS scenarios, the adaptation of the attack frequently takes place in a gradual change of the specific traffic attributes prior to significant changes globally. As a result, the study of feature level drift analysis is still largely under-explored and is potentially an important field that can improve the adaptive IDS. To tackle this problem, we propose FeDrift, a Feature-Level Drift Evolution Analysis framework for adaptive DDoS detection in dynamic networks that is capable of continuously monitoring feature evolution, quantifying the severity of feature drift, and enabling proactive detection of DDoS attacks. Apart from the distribution level, FeDrift also analyzes drift at the feature level, aiming to improve the robustness of the detection, explainability and adaptability of the dynamic network.

The main contributions of the paper are as follows:

- A Feature-Level Drift Evolution Analysis framework that characterizes temporal changes in network traffic using Wasserstein distance-based feature drift quantification.
- An adaptive drift detection mechanism that dynamically determines drift thresholds based on the statistical properties of evolving network traffic streams.
- An online adaptive DDoS detection architecture integrating drift monitoring with incremental learning classifiers for continuous model adaptation.
- An explainable analysis module to detect an influential drifting features that is affecting detection performance.

The remainder of this paper is organized as follows. Section II reviews related work on concept drift detection and adaptive intrusion detection systems. Section III presents the proposed FeDrift framework. Section IV describes the experimental setup and results. Finally, Section V concludes the paper and outlines future research directions.

2. Literature Review

Concept drift is a challenging problem in data stream mining since the distribution of data may change over time and this change can adversely affect the predictive performance. Gonçalves et al. [3] performed a comprehensive comparison study of drift detection methods such as Drift Detection Method (DDM), Early Drift Detection Method (EDDM), Page-Hinkley Test (PHT), Adaptive Windowing (ADWIN) , STEPD and Paired Learners and showed that no one detector is consistently the best for each drift scenario. Their study showed that they must be able to identify the drift early enough to preserve the effectiveness of the classifiers in non-stationary environments.

Recent research has concentrated on fully unsupervised drift detection in order to address the reliance on labeled data. Lukats et al. [2] took a look around and benchmarked various unsupervised detectors of which the most prominent ones were based on clustering, statistical testing, density estimation and distribution comparison. The researchers found that unsupervised approaches work especially well when continuous labelling is not feasible, as is the case in real-world streaming applications. Most of the methods are concerned with identifying drift events but not the changes at the feature level which cause the drift. Lara-Gutierrez et al. [1] highlighted that concept drift, feature drift and adversarial manipulations are some of the most significant challenges to AI-based threat detection systems in the cybersecurity sector.

Current methods are mostly based on detecting whether drift has occurred but do not have much insight into the evolution of individual network features and how it degrades the ability to detect drift. Seth et al. [8] proposed an adaptive IDS based on Adaptive Random Forest and ADWIN, enabling stream-oriented learning without repeated retraining. Their approach achieved high detection accuracy on CICIDS2018; however, adaptation remained dependent on classifier-level drift indicators rather than feature-level evolution. Similarly, Jemili et al. [9] combined concept drift detection with online incremental learning for intrusion detection demonstrating the feasibility of continuous model adaptation in streaming environments.

In the context of IoT security, Beshah et al. [10] introduced a drift-adaptive online DDoS detection framework employing an Accuracy Update Weighted Probability Averaging Ensemble (AUWPAE) mechanism. Their framework achieved high detection performance on IoTID20 and CICIoT2023 datasets while adapting to evolving attack patterns. Likewise, Selvam and Balasubramanian [11] proposed UASDAC, an unsupervised adaptive and scalable DDoS classification framework that incorporates concept drift detection and retraining strategies for large-scale IoT traffic streams.

Recent studies have explored more sophisticated drift-aware architectures. INSOMNIA [4] employed semi-supervised learning, active learning and explainable artificial intelligence to continuously update intrusion detection models under concept drift. CyberAdaptAI introduced an adaptive ensemble framework that dynamically adjusts classifier weights and triggers retraining through ADWIN-based drift detection [6].

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 06 , June - 2026

Researchers have also investigated alternative drift detection strategies. Chu et al. [12] proposed an ensemble of non-parametric localization detectors for identifying drift points in IoT data streams, while Chu et al. later introduced IF-DLDD, a double-layer drift detector based on Isolation Forest and statistical verification to reduce false alarms.

DDoS attack behaviors tend to manifest in a subtle way by evolving specific attribute of the traffic stream so knowledge of the feature evolution can help in earlier detection of attacks adapting to the network and in designing better model updates. This work thus proposes a feature-centric adaptive framework called FeDrift, which leverages a study of feature evolution patterns and feature drift dynamics to enhance the DDoS detection performance in ever changing network environments. Table 1 summarized the existing drift-aware DDoS detection frameworks.

Table 1. Summary of existing concept drift-aware DDoS detection frameworks

Reference	Method/Model	Dataset	Strengths	Limitations
[3]	DDM, EDDM, ADWIN, PHT	Synthetic and Real Data Streams	Comprehensive evaluation of drift detectors	Not designed for IDS/DDoS environments
[9]	Online Incremental Learning + Concept Drift Detection	Streaming Intrusion Data	Continuous online adaptation	Continuous online adaptation
[8]	Adaptive Random Forest + ADWIN	CICIDS2018	Online adaptation without frequent retraining	No feature-level analysis
[4]	INSOMNIA	Network Intrusion Streams	Robust against evolving attacks	Increased computational complexity
[10]	AUWPAE	IoTID20, CICIoT2023	High DDoS detection accuracy under drift	Ensemble complexity and computational cost
[6]	CyberAdaptAI	CICIDS2017, UNSW-NB15	Fast adaptation and recovery	Frequent retraining overhead
[5]	Learn-to-Adapt Drift Detection Framework	Cybersecurity Data Streams	Robust drift detection in security applications	Does not analyze feature-level evolution
[11]	UASDAC	IoT Networks	Scalable concept-drift-aware DDoS detection	Requires periodic adaptation
[12]	IF-DLDD	CICIDS2017	Low false alarms	Additional verification stage required

3. PROPOSED FEDRIFT FRAMEWORK

A. An overview

The proposed FeDrift framework is designed for adaptive DDoS detection in dynamic network environments. Unlike conventional IDS that rely on static learning assumptions, FeDrift continuously monitors feature distribution evolution over time, identifies significant concept drift events through adaptive thresholding and selectively adapts online classifiers to evolving traffic patterns. The framework comprises five major modules: (a) Stream Window Generation (b) Feature-level Drift Quantification (c) Adaptive Drift Detection (d) Selective Model Adaption and (e) Incremental DDoS Detection, which together form a unified drift-aware intrusion detection architecture, as shown in Fig. 1.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 06 , June - 2026

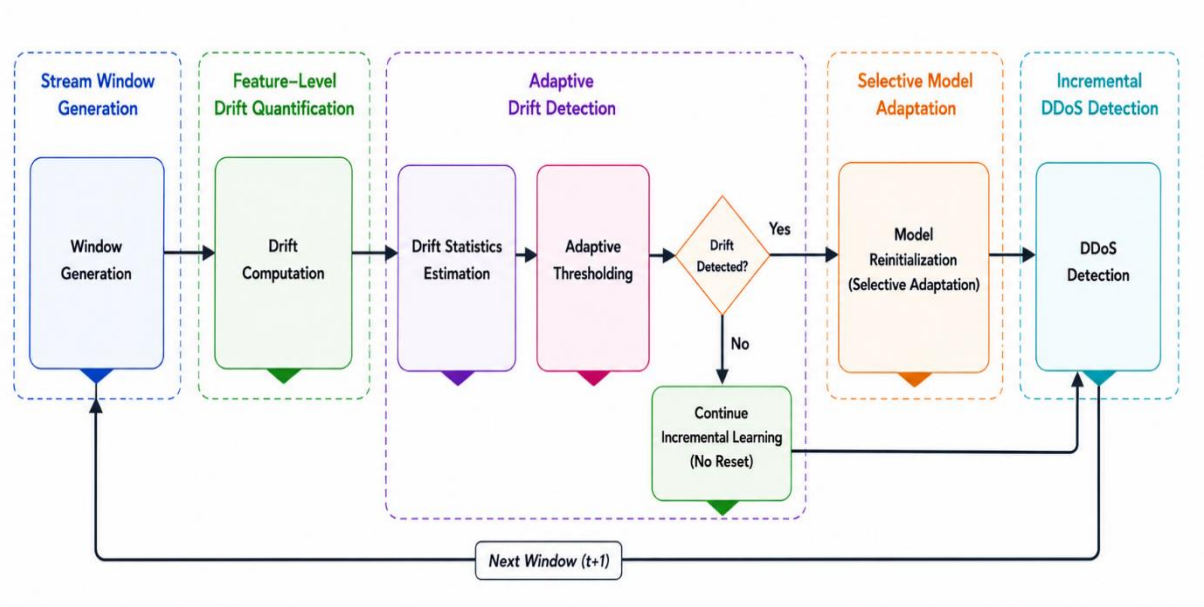

Fig.1. Operational workflow of proposed FeDrift framework

Network traffic is first partitioned into temporal windows, followed by feature-level drift analysis where feature distribution evolution between consecutive windows is quantified. Next by evaluating the drift characteristics of the current traffic window and dynamically adjusting the drift threshold significant concept evolution is separated from normal traffic fluctuations reducing false drift alarms. Upon detection of a significant drift event, the Selective Model Adaptation module performs model reinitialization to eliminate obsolete knowledge associated with previous traffic concepts and starts learning afresh from current concept. In the absence of drift, the framework preserves existing model knowledge and continues incremental learning without retraining. Finally, the Incremental Learning-based DDoS Detection module continuously updates the learning models using incoming traffic windows and generates online intrusion detection decisions.

B. The architecture

The overall architecture of the proposed framework is shown in Fig. 2. Each component performs a specific function within the drift-aware intrusion detection. Incoming network traffic is first transformed into a temporal stream representation and partitioned into consecutive windows. Feature-level drift is subsequently quantified using Wasserstein distance between consecutive windows. The resulting drift statistics are used to estimate an adaptive threshold capable of adjusting to evolving traffic behavior. Significant drift events trigger selective model adaptation while incremental classifiers continuously update their knowledge using newly arriving traffic windows. Finally, the framework produces DDoS detection decisions and comprehensive drift analytics for performance assessment.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 06 , June - 2026

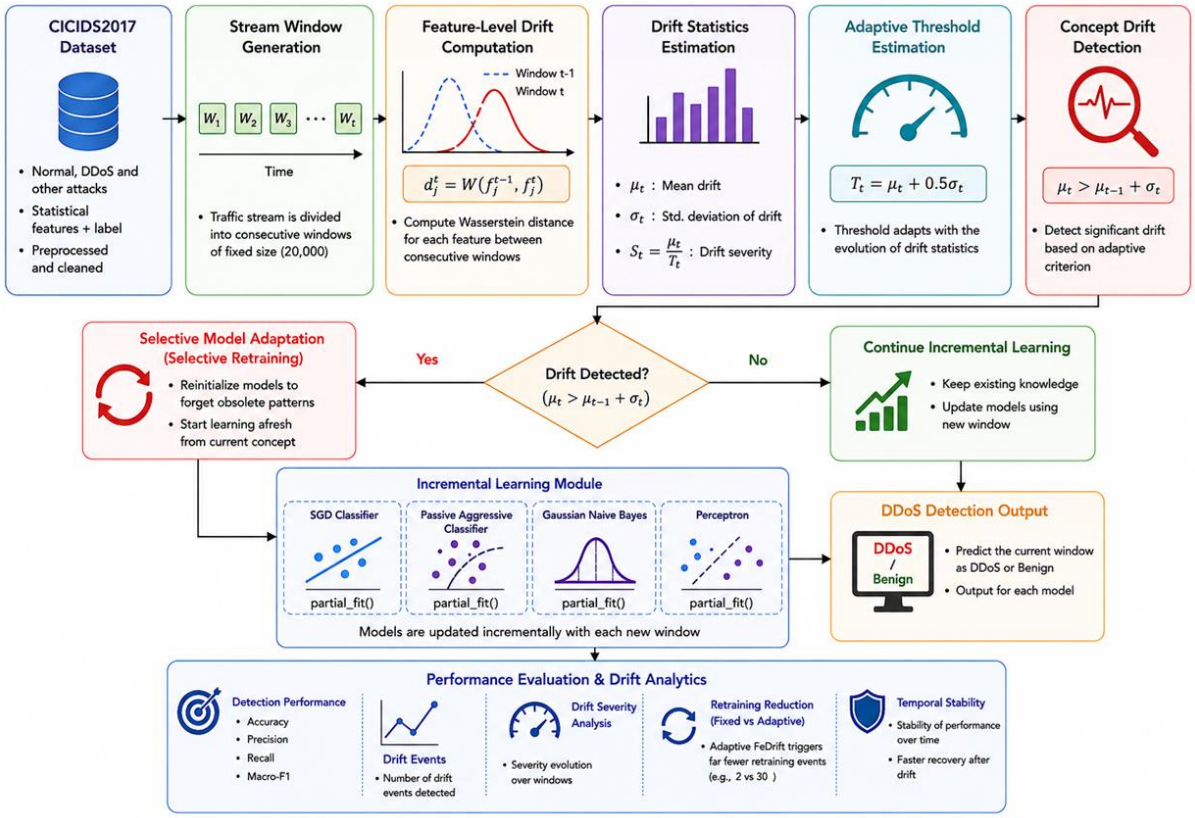

Fig. 2. The architecture of the proposed methodology

(i) Stream Window Generation

The Stream Window Generation partitions the incoming network traffic stream into consecutive temporal windows. Let the network traffic stream be represented as $\mathcal{S} = \{x_1, x_2, \ldots, x_N\}$ where x_i denotes an individual network traffic instance. To simulate a realistic streaming environment, the traffic stream is partitioned into consecutive non-overlapping windows $\mathcal{S} = \{W_1, W_2, \ldots, W_k\}$ where W_t denotes the traffic observations contained within the t^{th} temporal window. Windowing enables temporal monitoring of traffic evolution and facilitates drift analysis across consecutive traffic intervals.

(ii) Feature-Level Drift Analysis

FeDrift analyzes the evolution of individual traffic features by computing the Wasserstein distance between corresponding feature distributions in consecutive windows W_{t-1} and W_t. For feature f_j, the drift magnitude d_j^t at window t is computed as-

$$d_j^t = \mathcal{W}\left(f_j^{t-1}, f_j^t\right)$$

where $\mathcal{W}(\cdot)$ denotes the Wasserstein distance [13]. The Wasserstein distance between distributions $P$and $Q$is defined as

$$\mathcal{W}(P, Q) = \inf_{\gamma \in \Pi(P,Q)} \int \mid x - y \mid d\gamma(x, y)$$

where $\Pi(P, Q)$ denotes the set of all joint distributions having marginals P and Q. The Wasserstein metric is selected because it measures the minimum transportation cost required to transform one distribution into another making it highly effective for capturing gradual and abrupt distributional shifts in network traffic. The resulting feature drift vector is therefore

$$D_t = \{d_1^t, d_2^t, \ldots, d_n^t\}$$

where n represents the total number of network traffic features.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 06 , June - 2026

(iii) Drift Statistics Estimation

After obtaining the feature drift vector, FeDrift estimates the overall drift characteristics of the current window. The mean drift μ_t is computed as

$$\mu_t = \frac{1}{n}\sum_{j=1}^{n} d_j^t$$

while the standard deviation σ_t of drift is given by

$$\sigma_t = \sqrt{\frac{1}{n}\sum_{j=1}^{n}(d_j^t - \mu_t)^2}$$

Furthermore, drift severity S_t which measures the relative magnitude of drift with respect to the adaptive threshold, is quantified as

$$S_t = \frac{\mu_t}{T_t}$$

where T_t is adaptive drift threshold (defined later).

(iv) Adaptive Threshold Estimation

Traditional drift detection methods frequently employ static thresholds that remain fixed throughout the monitoring process. However, network traffic exhibits continuously evolving behavior making fixed thresholds prone to excessive false alarms or missed drift events. To address this limitation, FeDrift dynamically computes an adaptive threshold as

$$T_t = \mu_t + 0.5\sigma_t$$

The threshold automatically adjusts according to the observed drift distribution, enabling the framework to remain sensitive to significant changes while suppressing minor fluctuations.

(v) Concept Drift Detection

Concept drift is detected by comparing the current drift behavior with historical drift characteristics. A significant drift event is declared when

$$\mu_t > \mu_{t-1} + \sigma_t$$

where μ_{t-1} denotes the mean drift observed in the previous window. This adaptive criterion enables robust drift identification while avoiding excessive false drift alarms.

(vi) Selective Model Adaptation

Upon detecting a significant drift event, FeDrift selectively reinitializes the learning models. This mechanism prevents outdated traffic knowledge from influencing future predictions while avoiding unnecessary retraining during stable periods.

(vii) Incremental Learning-based DDoS Detection

Three incremental learning classifiers i.e. Stochastic Gradient Descent (SGD), Passive Aggressive (PA) and Gaussian Naïve Bayes (GNB) were employed as these models support online updates through *partial_fit()*, making them suitable for adaptive intrusion detection under streaming environments.

4. Experimental Results and discussion

4.1 Experimental Setup

The proposed FeDrift framework was evaluated using the CICIDS2017 dataset which is one of the most widely adopted benchmark datasets for intrusion detection research. Prior to model development, the dataset underwent a comprehensive preprocessing

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 06 , June - 2026

procedure that included the removal of missing and infinite values, categorical label encoding and Standard scalar normalization to ensure numerical stability and consistent feature representation across all traffic attributes.

To emulate real-time network monitoring, the pre-processed traffic stream was chronologically ordered and partitioned into consecutive non-overlapping windows of 20,000 instances each. Since the evolution of the features is to be analysed therefore no feature selection was performed.

4.2 Performance evaluation

To determine the performance of the classifiers traditional performance metrics like accuracy, precision, recall and false positive rate (FPR) have been evaluated shown in the Table 2.

Table 2. Performance evaluation of classifiers for the proposed adaptive FeDrift framework

Classifier	**Accuracy (%)**	**Precision (%)**	**Recall (%)**	**FPR (%)**
SGD	99.63	99.51	99.47	0.23
PA	99.71	99.51	99.68	0.27
GNB	93.81	89.79	95.78	8.01
Perceptron	99.69	99.52	99.62	0.25

The PA classifier achieved the highest overall performance with an accuracy of 99.71% and recall of 99.68%. The Perceptron and SGD classifiers exhibited comparable performance, achieving similar accuracies around 99.6%. In contrast, GNB produced lower performance with accuracy of 93.81% and a comparatively higher FPR of 8.01%. The superior performance of PA, SGD and Perceptron demonstrates the effectiveness of incremental learning combined with adaptive drift management for maintaining robust DDoS detection under evolving network traffic conditions.

4.3 Feature-Level Drift Evolution Analysis

To investigate the temporal evolution of network traffic characteristics, feature-level drift analysis was performed. Figure 3 illustrates the evolution of the mean feature drift and the corresponding adaptive threshold across successive traffic windows. The mean drift values exhibit noticeable fluctuations throughout the stream, indicating continuous variations in network traffic behaviour. However, the adaptive threshold dynamically adjusts according to the observed drift statistics, enabling the framework to distinguish substantial concept changes from normal traffic variations. As shown in the figure, significant drift events were detected only at windows 34 and 59 (shown in dotted blue lines), where the drift behaviour exceeded the adaptive detection criterion. The adaptive threshold successfully suppresses minor fluctuations while remaining sensitive to major distributional shifts, thereby reducing the likelihood of false drift alarms.

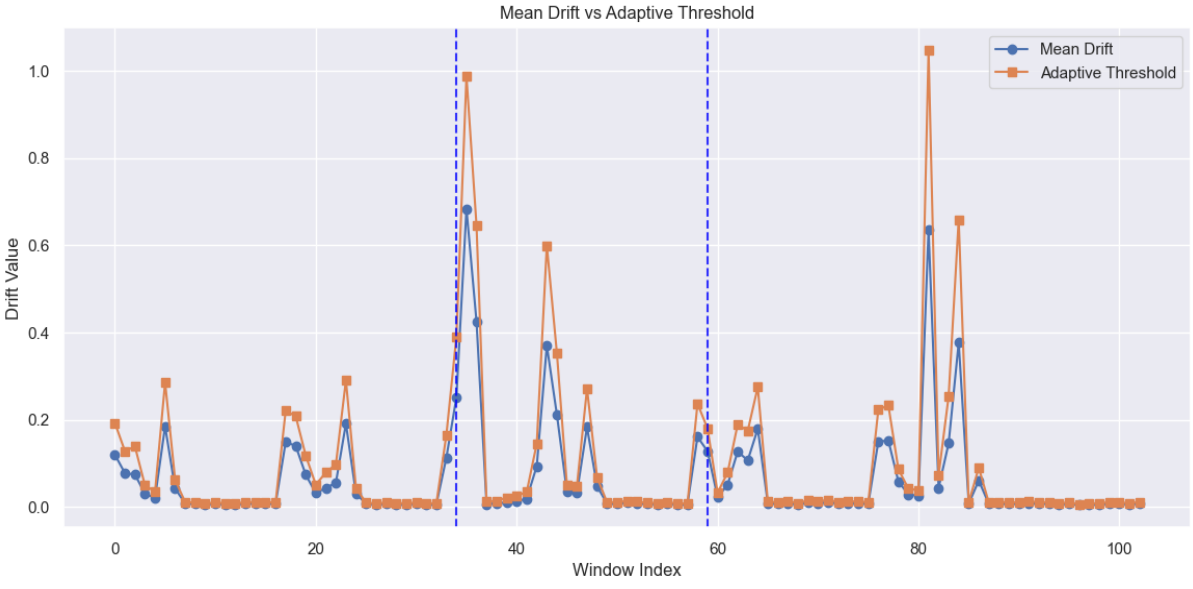

Fig. 3. Evolution of the mean feature drift and adaptive threshold

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 06 , June - 2026

Fig. 4. Temporal evolution of drift severity around windows

To further quantify the intensity of concept evolution, the drift severity score was evaluated for each traffic window. Figure 4 presents the temporal evolution of drift severity throughout the stream. Drift severity remains mostly between 0.55 and 0.78 throughout the stream ranging from 0 to 103 windows.

Upon realizing the heatmap in Figure 5, it can be seen that subset of features experiences substantial drift in the vicinity of windows 34–45 and 80–85. This suggests that concept evolution is primarily driven by a limited set of traffic characteristics rather than the entire feature space.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 06 , June - 2026

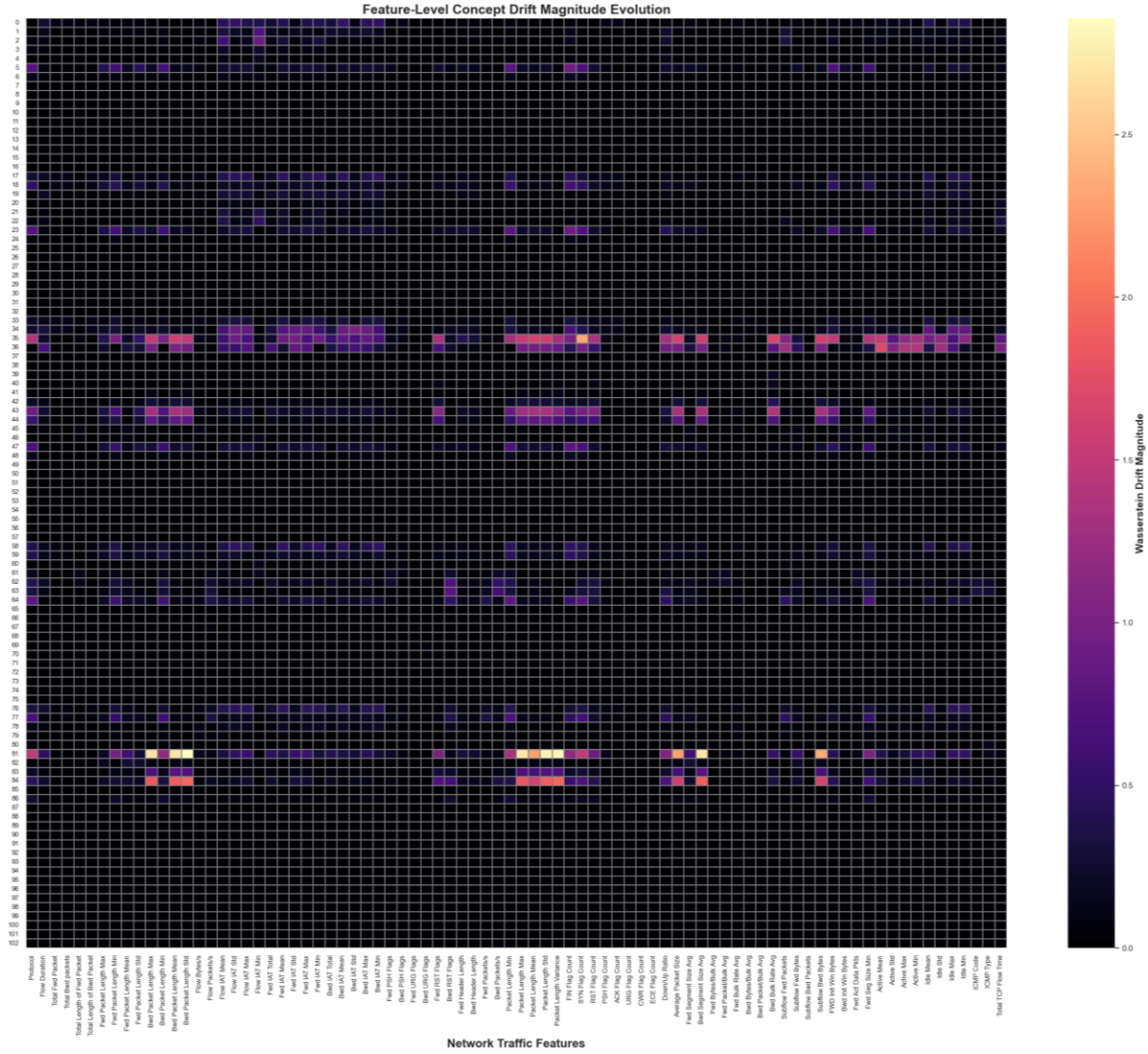

Fig. 5. Heatmap of traffic features

4.4 Adaptive Drift Detection and Model Stability Analysis

The effectiveness of the proposed adaptive drift detection mechanism was further evaluated by analysing the temporal evolution of classifier performance across all traffic windows. Figures 6 and 7 illustrate the window-wise Macro-F1 score and classification accuracy, respectively, with the detected drift events indicated at windows 34 and 59.

It can be observed that the SGD, PA and Perceptron classifiers maintained consistently high performance throughout the stream, despite the occurrence of concept drift. The Macro-F1 and accuracy values remained close to unity for most windows, indicating strong resilience to evolving traffic distributions. Although minor performance fluctuations were observed around the detected drift regions, the classifiers rapidly stabilized without exhibiting significant degradation.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 06 , June - 2026

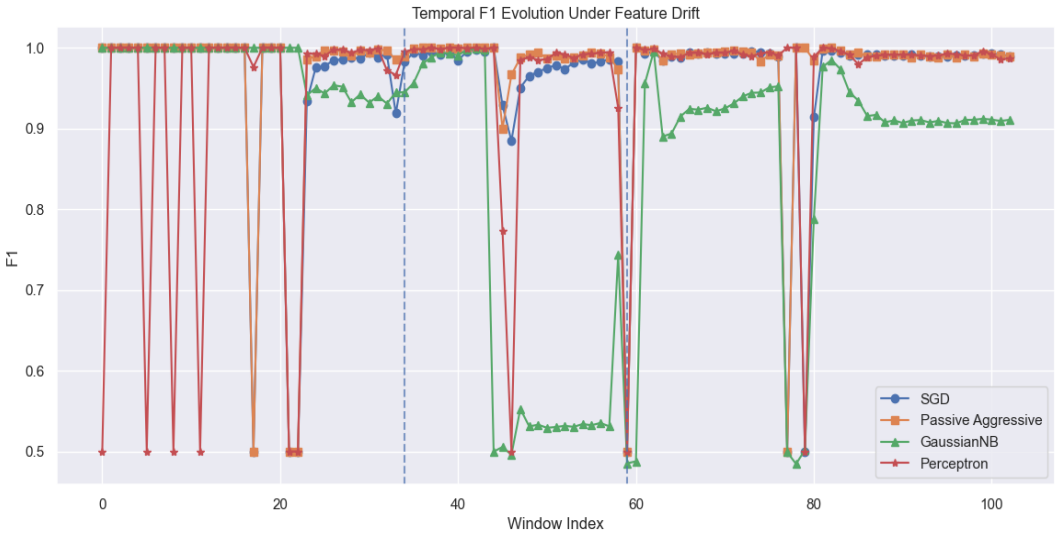

Fig. 6. Temporal f1 evolution of classifiers

In contrast, the GNB demonstrated comparatively larger fluctuations in both Macro-F1 and accuracy, suggesting higher sensitivity to changes in feature distributions. Nevertheless, the overall results indicate that the proposed FeDrift framework effectively manages concept drift while preserving stable detection performance over time. The observed temporal stability confirms the capability of the adaptive drift detection and selective model adaptation mechanisms to maintain classifier effectiveness under continuously evolving network traffic conditions (see figs. 6 and 7).

Fig. 7. Temporal accuracy evolution of classifiers

4.4 Adaptive versus Fixed Threshold Analysis

To evaluate the effectiveness of the proposed adaptive drift detection mechanism, FeDrift was compared against a conventional fixed-threshold baseline using an identical experimental configuration. The fixed-threshold approach employed a constant drift threshold of 0.25 throughout the traffic stream. The fixed-threshold strategy detected 30 drift events across the network traffic stream resulting in frequent model reinitializations and repeated adaptation cycles. In contrast, the proposed FeDrift framework identified only two significant drift events at windows 34 and 59. This corresponds to a 93.33% reduction in drift-triggered model adaptations, indicating that the adaptive threshold successfully distinguished meaningful concept evolution from normal traffic fluctuations (see fig. 8).

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 06 , June - 2026

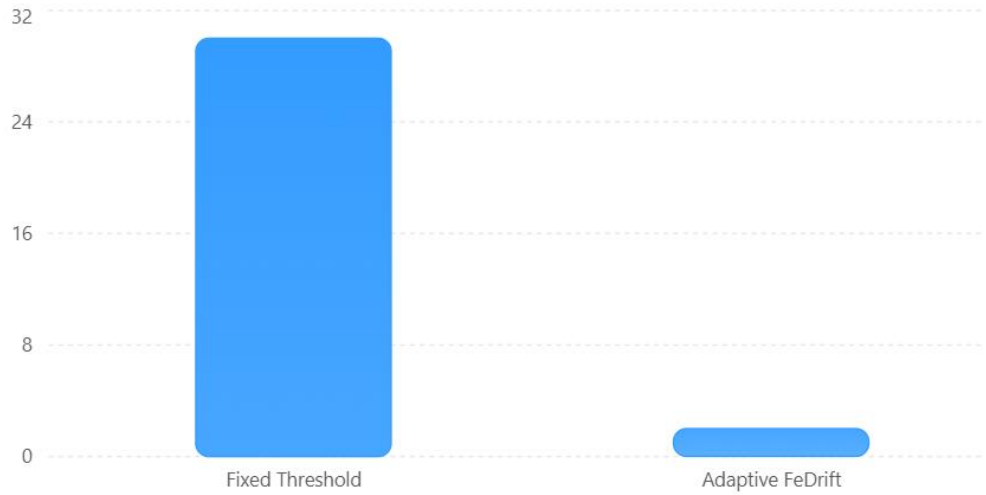

Fig. 8. Drift event comparison

Despite the substantial reduction in adaptation frequency, the detection performance of the incremental learning classifiers remained largely unchanged. The PA classifier achieved the highest Macro-F1 score of 0.9960 under the adaptive setting, followed by the Perceptron (0.9957) and SGD (0.9949) classifiers. Compared with the fixed-threshold baseline, the differences in performance were negligible for SGD, PA, and Perceptron, demonstrating that excessive retraining was not necessary to maintain high DDoS detection accuracy.

Table 3. Macro-F1 comparison between fixed-threshold and adaptive-threshold

Model	**Fixed**	**Adaptive**
SGD	99.51	99.49
PA	99.58	99.60
GNB	96.50	92.16
Perceptron	99.49	99.57

5. CONCLUSION AND FUTURE SCOPE

This paper presented FeDrift, an adaptive drift-aware framework for DDoS detection in evolving network environments. The proposed framework integrates feature-level drift quantification, adaptive threshold-based drift detection, selective model adaptation, and incremental learning into a unified intrusion detection architecture. Experimental results on the CICIDS2017 dataset demonstrated that the proposed approach effectively identifies significant concept drift while maintaining high detection performance. The adaptive mechanism detected only two major drift events and reduced drift-triggered model adaptations by 93.33% compared with a fixed-threshold approach. Among the evaluated classifiers, the Passive Aggressive classifier achieved the best overall performance, confirming the effectiveness of the proposed framework for adaptive intrusion detection.

Future work will focus on incorporating adaptive feature selection and ensemble-based incremental learning strategies to further improve drift handling capabilities.

Contribution

Amrendra Kumar Sharma has offered the proposed FeDrift framework, performed experiments, analyzed results and prepared the manuscript. Dr. Mamta Tiwari supervised the study, reviewed the methodology and results and contributed in manuscript revision for final approval.

Conflict of Interest

The authors declare that they have no known competing financial or non-financial interests that could have influenced the work reported in this study.

Funding Declaration

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 06 , June - 2026

This research received no external funding.

REFERENCES

[1] A. Lara-Gutierrez, C. Fernandez-Gago, and J. A. Onieva, "A Framework for Drift Detection and Adaptation in AI-driven Anomaly and Threat Detection Systems: A. Lara-Gutierrez et al.," *Int. J. Inf. Secur.*, vol. 24, no. 5, p. 199, 2025.

[2] D. Lukats, O. Zielinski, A. Hahn, and F. Stahl, "A benchmark and survey of fully unsupervised concept drift detectors on real-world data streams," *Int. J. Data Sci. Anal.*, vol. 19, no. 1, pp. 1–31, 2025.

[3] P. M. Gonçalves Jr, S. G. T. de Carvalho Santos, R. S. M. Barros, and D. C. L. Vieira, "A comparative study on concept drift detectors," *Expert Syst. Appl.*, vol. 41, no. 18, pp. 8144–8156, 2014.

[4] G. Andresini, F. Pierazzi, and L. Cavallaro, *INSOMNIA : Towards Concept-Drift Robustness in Network Intrusion Detection*, vol. 1, no. 1. Association for Computing Machinery, 2021. doi: 10.1145/3474369.3486864.

[5] A. Kuppa, "Learn to adapt : Robust drift detection in security domain ☆," *Comput. Electr. Eng.*, vol. 102, no. August, p. 108239, 2022, doi: 10.1016/j.compeleceng.2022.108239.

[6] N. Uddamari and P. Sammulal, "CyberAdaptAI : A Dynamic Ensemble Learning Framework for Real-Time Cyberattack Detection Using AdaptEnsembleNet," vol. 12, no. 9, pp. 11–31, 2025.

[7] R. B. Sebopelo, "Trinity-Controller ADWIN : An Accuracy Guided Sensitivity Control Framework for Streaming Intrusion Detection," vol. 8, no. 1, pp. 501–529, 2026.

[8] S. Seth, G. Singh, and K. Kaur, "Drift-based approach for evolving data stream classification in Intrusion detection system," pp. 0–3, 2021.

[9] F. Jemili, "Intrusion Detection based on Concept Drift Detection & Online Incremental Learning," 2023.

[10] Y. K. Beshah and S. L. Abebe, "Drift Adaptive Online DDoS Attack Detection Framework for IoT System," 2024.

[11] U. M. A. M. Balasubramanian, "UASDAC : An Unsupervised Adaptive Scalable DDoS Attack Classification in Large-Scale IoT Network Under Concept Drift," *IEEE Access*, vol. 12, no. May, pp. 64701–64716, 2024, doi: 10.1109/ACCESS.2024.3397512.

[12] R. Chu, M. Luo, L. Yang, J. Xiao, and Y. Liao, "Concept Drift Analysis Based on Isolation Forest for Effectively Detecting Network Attack in IoT Scenarios," *IEEE Access*, vol. 14, no. December 2025, pp. 3245–3258, 2026, doi: 10.1109/ACCESS.2025.3650576.

[13] G. Peyré and M. Cuturi, *Computational optimal transport: With applications to data science*. Now Foundations and Trends, 2019.