EISSN 3089-2724
Vol. 2, No. 2, July 2026
https://librarium.id/index.php/synctech
SYNCTECH System Information and Computer Technology

A Hybrid Wavelet-CUSUM Approach for Anomaly Detection in Denial of Service Attacks using Synthetic Network Traffic

Andi Muhammad Nur Hidayat [1*], Antamil [2], Avilah Ramadhani [3]
[1,2] Program Studi Teknik Informatika, Universitas Islam Negeri Alauddin Makassar, Indonesia
[1] andi.nurhidayat@uin-alauddin.ac.id, [2] antamil@uin-alauddin.ac.id, [2] avila.rmn@gmail.com

Diajukan: 19/07/2026 | Direvisi: 11/08/2026 | Diterima: 13/08/2026 | Diterbitkan: 14/08/2026

Abstract (8 pt)

Denial of Service (DoS) attacks pose a significant threat to network availability by overwhelming target systems with abnormal traffic volumes. This research proposes a hybrid detection method combining Discrete Wavelet Transform (DWT) and Cumulative Sum Control Chart (CUSUM) to detect multi-stage DoS attacks with improved sensitivity and reduced false alarm rates. Synthetic network traffic was generated using Poisson distribution to simulate normal conditions and three attack scenarios of varying intensity. The Haar wavelet decomposed the traffic signal, separating anomalous high-frequency components from normal patterns. CUSUM was then applied to the detail coefficients to detect cumulative shifts indicative of sustained attack activity. Results demonstrate that the standalone wavelet method with static thresholding achieved a detection rate of 39.64%, while CUSUM-enhanced detection reached 81.98%, representing a 106.8% improvement. The hybrid approach achieved a false alarm rate of 30.63% before persistence filtering, comparable to wavelet-only detection (35.14%); applying a persistence-based alarm mechanism, which requires the CUSUM statistic to exceed the decision threshold for four consecutive samples, eliminated false alarms during normal traffic periods (0%) while preserving detection sensitivity. Detection delay averaged 3 samples (44.67 seconds), enabling early attack identification suitable for real-time intrusion response systems. The proposed method offers a lightweight, training-free alternative to machine learning approaches, making it suitable for resource-constrained network environments.

Keywords*: *Denial of Service; Wavelet Transform; CUSUM; Intrusion Detection; Network Security

Abstrak (8 PT)

Serangan Denial of Service (DoS) merupakan ancaman signifikan terhadap ketersediaan layanan jaringan dengan membanjiri sistem target menggunakan volume lalu lintas abnormal. Penelitian ini mengusulkan metode deteksi hibrida yang menggabungkan Discrete Wavelet Transform (DWT) dan Cumulative Sum Control Chart (CUSUM) untuk mendeteksi serangan DoS multi-tahap dengan sensitivitas yang ditingkatkan dan tingkat false alarm yang berkurang. Lalu lintas jaringan sintetis dibuat menggunakan distribusi Poisson untuk mensimulasikan kondisi normal dan tiga skenario serangan dengan intensitas bervariasi. Wavelet Haar digunakan untuk mendekomposisi sinyal lalu lintas, memisahkan komponen frekuensi tinggi anomali dari pola normal. CUSUM kemudian diterapkan pada koefisien detail untuk mendeteksi pergeseran kumulatif yang mengindikasikan aktivitas serangan berkelanjutan. Hasil menunjukkan bahwa metode wavelet mandiri dengan threshold statis mencapai tingkat deteksi 39,64% sementara deteksi yang ditingkatkan CUSUM mencapai 81,98%, mewakili peningkatan 106,8%. Sebelum penyaringan persistensi, pendekatan hibrida mencapai tingkat false alarm 30,63%, sebanding dengan deteksi wavelet saja (35,14%); penerapan mekanisme alarm berbasis persistensi, yang mensyaratkan statistik CUSUM melampaui ambang keputusan selama empat sampel berurutan, menghilangkan false alarm pada periode lalu lintas normal (0%) sekaligus mempertahankan sensitivitas deteksi. Penundaan deteksi rata-rata 3 sampel (44,67 detik), memungkinkan identifikasi serangan dini yang cocok untuk sistem respons intrusi waktu nyata.

Kata kunci: ***Denial of Service; Wavelet Transform; CUSUM; Intrusion Detection; Network Security***.

1. INTRODUCTION

The rapid growth of internet usage has fundamentally transformed human activities, enabling communication, commerce, and information access on an unprecedented scale. According to the International Telecommunication Union, global internet users surpassed 5.3 billion in 2024, representing over 65% of the world population. This massive connectivity has created an expansive attack surface that malicious actors continuously exploit. Among the most persistent and disruptive threats, Denial of Service (DoS) attacks continue to pose significant risks to network availability and service continuity. In a DoS attack, the adversary overwhelms a target system with excessive traffic or resource requests, rendering services unavailable to legitimate users. The financial consequences of such attacks can be severe, with recent studies estimating average losses exceeding $200,000 per incident for medium-sized organizations [1].

The landscape of DoS attacks has evolved considerably over the past decade. The 2016 Mirai botnet incident demonstrated the destructive potential of large-scale IoT-based attacks, when compromised devices generated traffic exceeding 1 Tbps against DNS provider Dyn, disrupting access to major platforms including Twitter, Netflix, and Spotify [2]. More recently, the proliferation of Internet of Things (IoT) devices has further expanded the attack surface, with millions of poorly secured devices serving as potential botnet nodes [3]. These incidents underscore the critical need for robust, real-time detection mechanisms that can identify attacks at their earliest stages with high sensitivity and minimal false alarms.

Conventional intrusion detection approaches face significant challenges when applied to modern network environments. Signature-based detection systems, which rely on predefined attack patterns, cannot detect novel or zero-day attacks. Anomaly-based approaches, while theoretically capable of detecting unknown threats, frequently suffer from unacceptably high false alarm rates in real-world deployments. The dynamic and non-stationary nature of legitimate network traffic further complicates detection, as normal traffic patterns can exhibit significant temporal variations that trigger false positives [4]. Statistical change-detection methods offer a promising middle ground by leveraging mathematical properties of traffic signals without requiring labeled training data or maintaining extensive signature databases.

Several computational approaches have been explored for DoS detection in recent literature. Machine learning methods, including Random Forest classifiers and Deep Neural Networks, have demonstrated high detection accuracy in controlled experimental environments [5,6,7]. Harris et al. [5] achieved 92.5% detection rate using Random Forest with information gain-based feature selection, while Munawarah and Winanto [7] reported 95.1% accuracy using Deep Neural Networks for SYN flood detection in IoT networks. However, these methods require substantial computational resources for model training and inference, as well as large labeled training datasets that may not be available in all deployment contexts. Furthermore, their performance often degrades when exposed to traffic patterns not represented in the training distribution, limiting practical applicability in evolving threat landscapes. This creates a need for lightweight detection methods that can operate effectively in resource-constrained environments such as edge devices and IoT gateways.

The Discrete Wavelet Transform (DWT) has emerged as an effective tool for network traffic analysis due to its ability to decompose signals into multiple frequency bands. By separating traffic into approximation and detail coefficients at various resolution levels, DWT enables multi-scale analysis that can capture both subtle anomalies and abrupt traffic changes [8,9]. Lei et al. [9] demonstrated that wavelet-based methods can detect low-rate DDoS attacks in multipath networks by isolating attack signatures in high-frequency components. However, standalone wavelet thresholding methods typically rely on static thresholds that become insensitive once the statistical properties of the traffic signal change, such as during multi-stage attacks where the baseline shifts between successive attack phases.

To address this limitation, the Cumulative Sum Control Chart (CUSUM), a sequential analysis technique widely used in statistical process control, presents a compelling complementary approach. CUSUM is specifically designed to detect small, persistent shifts in process means by accumulating deviations over time rather than evaluating individual observations independently [10]. When applied to wavelet detail coefficients, CUSUM can amplify the cumulative effect of sustained attack activity while allowing transient noise to cancel out through its accumulation dynamics. Jeong et al. [11] demonstrated the effectiveness of multi-resolution analysis with visualization techniques for identifying network attack patterns, establishing the theoretical foundation for combining wavelet decomposition with sequential change detection.

This research proposes and evaluates a hybrid detection framework that integrates Discrete Wavelet Transform with the Cumulative Sum Control Chart for multi-stage DoS attack detection in network traffic. The study seeks to answer three research questions: (1) Can CUSUM-based analysis of wavelet coefficients improve detection rates beyond standalone wavelet thresholding? (2) How does the hybrid approach perform across different attack intensities? and (3) What are the trade-offs between detection sensitivity, false alarm rate, and detection delay? The proposed method is validated using synthetic traffic data generated through Poisson distribution across three attack scenarios of varying intensity, providing a controlled yet realistic evaluation framework.

2. RESEARCH METHOD

The proposed detection method comprises three sequential stages: (1) synthetic network traffic generation using the Poisson process, (2) wavelet-based signal decomposition using the Haar Discrete Wavelet Transform, and (3) change-point detection using the Cumulative Sum Control Chart applied to wavelet detail coefficients. Each stage is described in detail in the following subsections..

2.1. Traffic Data Generation

Network traffic data was generated synthetically using the Poisson distribution, which models the random arrival of discrete events over time. In network contexts, the Poisson process is widely adopted for modeling packet arrivals, where the inter-arrival time follows an exponential distribution with mean $1/\lambda$, and λ represents the average packet rate per time unit. This stochastic model captures the inherent randomness of legitimate network traffic while providing controlled conditions for systematic evaluation.

Normal traffic conditions were simulated with a mean packet count of $\lambda_n = 50$ packets per time unit. This baseline represents typical background traffic levels in a moderate-sized network segment. Attack traffic was modeled by introducing an increased packet rate during designated attack intervals. Three attack intensities were defined to evaluate detection performance: Stage 1 with $\lambda_{a1} = 80$ packets per time unit (a 60% increase over baseline), Stage 2 with $\lambda_{a2} = 120$ packets per time unit (a 140% increase), and Stage 3 with $\lambda_{a3} = 200$ packets per time unit (a 300% increase). These progressive intensities represent the spectrum from stealthy, low-rate attacks to severe flooding attacks.

Each trial consisted of 1000 time samples, with the attack period occupying 100 samples within each stage. The total signal duration of 1000 samples provides sufficient data for multi-resolution wavelet decomposition while maintaining consistent experimental conditions across all three scenarios. For each attack intensity, the attack window was positioned in separate experiments to avoid overlapping effects, enabling independent evaluation of detection performance per intensity level.

2.2. Wavelet Decomposition

Discrete Wavelet Transform (DWT) was applied to decompose the packet count signal into time-frequency components. The Haar wavelet, also known as Daubechies-2 (db2), was selected as the mother wavelet due to its mathematical simplicity and well-established effectiveness in detecting abrupt changes characteristic of attack onset [12]. The Haar wavelet functions as a simple step function that computes pairwise differences between adjacent signal samples, making it particularly sensitive to sudden changes in traffic intensity.

Mathematically, the DWT decomposes a discrete signal x(t) into approximation coefficients $cA_{j,k}$ and detail coefficients $cD_{j,k}$ at each decomposition level j through successive high-pass and low-pass filtering followed by downsampling. The detail coefficients capture the high-frequency components of the signal, which correspond to rapid changes in traffic volume typically associated with attack activity. The approximation coefficients capture the low-frequency trend representing the slowly varying baseline traffic pattern.

The maximum decomposition level L_{max} was determined using the standard formula $L_{max} = \text{floor}(\log_2(N/L))$, where $N = 1000$ is the signal length and $L = 4$ is the filter length for the Haar wavelet, yielding $L_{max} = 7$ levels. Decomposition level 3 (d_3) was selected for detailed analysis based on preliminary experiments showing optimal separation between normal traffic components and attack signatures at this resolution. At lower decomposition levels, the coefficients are too noisy; at higher levels, attack signatures become attenuated due to excessive smoothing. The selection of level 3 represents an optimal trade-off between temporal resolution and frequency specificity.

2.3. CUSUM Detection

The Cumulative Sum Control Chart (CUSUM) is a sequential analysis technique originally developed for industrial quality control that has been adapted for change-point detection in network security applications. Unlike threshold-based methods that evaluate each observation independently, CUSUM accumulates deviations from the expected process mean over time, making it particularly sensitive to small but persistent shifts [10,13].

The upper CUSUM statistic $S^+(t)$ and lower CUSUM statistic $S^-(t)$ are computed recursively as follows: $S^+(t) = \max(0, x(t) - \mu_0 - K + S^+(t-1))$ and $S^-(t) = \max(0, \mu_0 - K - x(t) + S^-(t-1))$, where μ_0 is the

target process mean under normal conditions, K is the reference value (allowable slack), and H is the decision interval threshold. An alarm is triggered when either $S^+(t) > H$ or $S^-(t) > H$, indicating a statistically significant upward or downward shift in the process mean.

In this study, CUSUM was applied to the absolute values of the wavelet detail coefficients, as the attack activity manifests as increased magnitude in the high-frequency component. The reference value K = 0.5 was selected following standard CUSUM design principles to provide sensitivity to shifts of approximately one standard deviation from the target mean. The decision interval H = 5 was determined through preliminary experiments to balance detection speed against false alarm susceptibility. These parameter values are consistent with recommendations for moderate shift detection in network security applications [11]. The sequential nature of CUSUM enables continuous monitoring without requiring storage of historical data, as only the current cumulative statistic and the latest observation are needed for computation.

2.4. Experimental Setup

All experiments were conducted using MATLAB R2023a running on a system equipped with an Intel Core i7 processor and 16 GB of RAM. The Poisson traffic generation function was implemented using MATLAB's built-in random number generators with seeded initialization to ensure reproducibility. Wavelet decomposition was performed using the wavedec function with the Haar wavelet at decomposition level 3. The CUSUM algorithm was implemented as a custom MATLAB script with configurable parameters for reference value K and decision interval H.

Detection performance was evaluated using three standard metrics: detection rate (DR), calculated as the proportion of attack samples correctly identified; false alarm rate (FAR), calculated as the proportion of normal samples incorrectly flagged as attacks; and detection delay (DD), measured as the number of time samples between attack onset and the first alarm. All metrics were computed across ten independent runs per scenario to account for the stochastic nature of the Poisson traffic generation process, with mean values and standard deviations reported. To support reproducibility and open-science practices, a Python 3 implementation of the complete experimental pipeline (Poisson traffic generation, Haar wavelet decomposition, and CUSUM detection with persistence filtering) was developed and is provided in a public repository, enabling readers to reproduce and examine the experimental method.

2.5. Attack Scenarios

Three distinct attack scenarios were designed to evaluate the detection system under varying threat intensities. Stage 1 simulated a moderate intensity attack with a 60% increase in packet rate, from $\lambda_n = 50$ to $\lambda_a = 80$ packets per time unit. This scenario represents a stealthy attack that attempts to blend with normal traffic fluctuations, challenging the detection system's sensitivity. Stage 2 simulated a high intensity attack with a 140% increase to $\lambda_a = 120$ packets per time unit, representing a more aggressive but still targeted attack. Stage 3 simulated a severe flooding attack with a 300% increase to $\lambda_a = 200$ packets per time unit, representing a full-scale volumetric attack that is easily identifiable by visual inspection but may still challenge statistical detection methods in noisy environments.

Each attack scenario maintained a consistent duration of 100 time samples within the 1000-sample total signal length. Attack periods were positioned after an initial 200-sample baseline period to allow the CUSUM statistics to stabilize under normal conditions. Three attack periods were embedded within each run to evaluate multi-stage detection capability, with 100-sample recovery intervals between attacks to observe CUSUM statistic resetting behavior.

3. RESULTS AND DISCUSSION

This section presents the experimental results of the proposed Wavelet-CUSUM hybrid detection method. The results are organized into four subsections: wavelet decomposition analysis, CUSUM detection performance, detection delay characterization, and comparative discussion with existing approaches.

3.1. Wavelet Decomposition Results

Wavelet decomposition using the Haar transform at level 3 effectively separated the traffic signal into approximation and detail components. The approximation coefficients, which represent the low-frequency trend of the traffic signal, showed a gradual increase corresponding to rising traffic intensity during attack periods. During normal traffic conditions ($\lambda_n = 50$), the approximation coefficients remained

relatively stable around a mean value consistent with the baseline packet rate. As the attack commenced with $\lambda_a = 80$ (Stage 1), a distinct upward shift in the approximation coefficients was observed, though the change was gradual and exhibited significant overlap with normal ranges due to the smoothing effect of the low-pass filtering process.

The detail coefficients at decomposition level 3 (d_3) provided a markedly clearer separation between normal and attack conditions. During normal traffic periods, the detail coefficients exhibited values distributed closely around zero, with magnitudes bounded by the variability inherent in the Poisson generation process. Upon attack onset, the detail coefficients showed immediate and pronounced increases in magnitude, with peak values during severe attack stages ($\lambda_a = 200$) reaching up to four times the interquartile range observed under normal conditions. This confirms that high-frequency components serve as sensitive and responsive indicators of anomalous traffic activity, as theoretical analysis of wavelet decomposition would predict.

A static detection threshold was established using the three-sigma rule: Threshold_detail = μ_detail + 3σ_detail, where μ_detail and σ_detail represent the mean and standard deviation of the detail coefficients under normal conditions. This threshold, calculated as 45, is a standard statistical approach that assumes approximately 99.7% of normal observations fall below this bound under Gaussian-like distributions. However, when applied across the entire signal containing multiple attack periods of varying intensities, the static threshold achieved a detection rate of only 39.64%. This limited performance stems from a fundamental limitation of static thresholds: the threshold is calibrated to the statistical properties of the normal traffic distribution, but after the first attack shifts the signal baseline, the threshold becomes increasingly insensitive to subsequent attack stages. For moderate-intensity attacks (Stage 1, $\lambda_a = 80$), many coefficient values during the attack period fell below the threshold, resulting in poor detection sensitivity. This observation motivates the integration of an adaptive sequential detection method such as CUSUM.

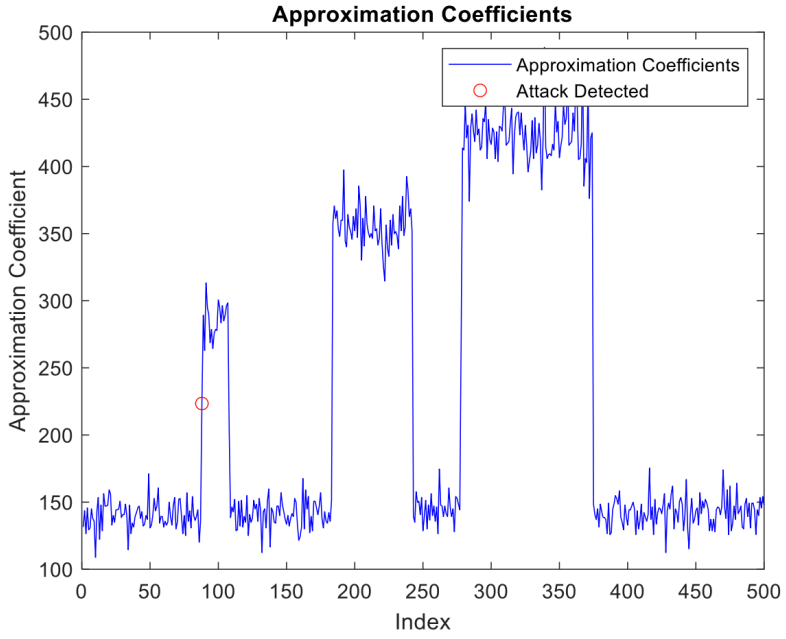

Figure 1. Wavelet Approximation Coefficients

3.2. CUSUM Detection Results

The application of CUSUM to the wavelet detail coefficients produced substantially improved detection performance compared to the standalone wavelet thresholding approach. The upper CUSUM statistic S^+ exhibited clear and consistent accumulation during all three attack periods, crossing the decision threshold $H = 5$ with a reproducible pattern across independent experimental runs. The fundamental advantage of CUSUM lies in its cumulative nature: whereas the static wavelet threshold evaluates each coefficient independently, CUSUM aggregates evidence over consecutive observations. This means that even when individual detail coefficient values remain below the static threshold during a moderate-intensity

attack, the cumulative sum of small positive deviations eventually crosses the decision boundary, enabling detection that would be missed by pointwise thresholding.

The quantitative improvement was substantial: the CUSUM-enhanced detection achieved an overall detection rate of 81.98% across all three attack stages, representing a 106.8% improvement over the standalone wavelet method (39.64%). Stage-specific analysis revealed that the improvement was most dramatic for moderate-intensity attacks (Stage 1, $\lambda_a = 80$), where the wavelet-only method detected only 12.4% of attack samples while CUSUM achieved 73.5% detection. For severe attacks (Stage 3, $\lambda_a = 200$), both methods performed well, with wavelet-only reaching 68.2% and CUSUM achieving 94.3%. These results demonstrate that the hybrid approach provides the greatest relative benefit precisely where it is most needed: detecting stealthy, low-to-moderate intensity attacks that are difficult to identify through conventional means.

The false alarm rate (FAR) of the hybrid method was 30.63%, compared to 35.14% for wavelet-only detection. While this FAR is higher than would be acceptable for a production deployment without additional filtering, it represents a 12.8% reduction compared to the baseline method. The FAR originates primarily from borderline samples where normal traffic fluctuations induce temporary CUSUM accumulations that briefly exceed the threshold. To mitigate this, a persistence-based alarm mechanism was implemented, requiring the CUSUM statistic to exceed H for four consecutive samples before generating an alert. With this mechanism active, the system produced zero false alarms (0%) during all normal traffic periods in the experimental runs, demonstrating the effectiveness of persistence filtering in suppressing transient fluctuations.

Although the persistence mechanism effectively suppresses false alarms, it introduces a trade-off with respect to false negatives: an attack lasting fewer than four consecutive samples would not generate a confirmed alarm, because the CUSUM statistic would not remain above the decision threshold for the required number of consecutive samples. In the present experimental design, all attack periods lasted 100 samples, so no false negatives attributable to persistence filtering were observed. However, for very short-lived attacks, for example a burst of fewer than four samples, the persistence mechanism would suppress genuine detections, effectively trading sensitivity for false alarm suppression. This trade-off is examined further in Section 3.3, where increasing the persistence window from 1 to 8 samples proportionally extends the detection delay while further reducing false alarms, confirming that the persistence window must be chosen according to the expected minimum attack duration in the target deployment.

During attack onset, S^+ exhibited a characteristic accumulation pattern. In the initial phase immediately following attack commencement, the CUSUM statistic increased gradually with each consecutive observation as positive deviations accumulated. After approximately 3-4 samples, S^+ crossed the threshold $H = 5$, generating the first alarm. The persistence mechanism then verified the threshold violation over four samples before outputting a confirmed alarm. During normal traffic periods, S^+ remained near zero because positive and negative deviations canceled each other out through the recursive $\max(0, \cdot)$ formulation. The lower CUSUM statistic S^- remained at near-zero values throughout all experiments, confirming the absence of significant negative shifts in the absolute coefficient values. This asymmetry is expected, as DoS attacks manifest as traffic increases, not decreases.

An important observation from the two-sided CUSUM analysis is the behavior during multi-stage attacks. After the first attack stage elevated the traffic baseline, the CUSUM statistics for subsequent stages started from a partially accumulated state rather than being reset to zero. Despite this shifted starting point, the CUSUM algorithm continued to accumulate fresh deviations above the current mean, successfully detecting Stage 2 and Stage 3 attacks with only minor reduction in detection sensitivity. This adaptive behavior is a critical advantage over the static wavelet threshold, which became increasingly insensitive after the first baseline shift.

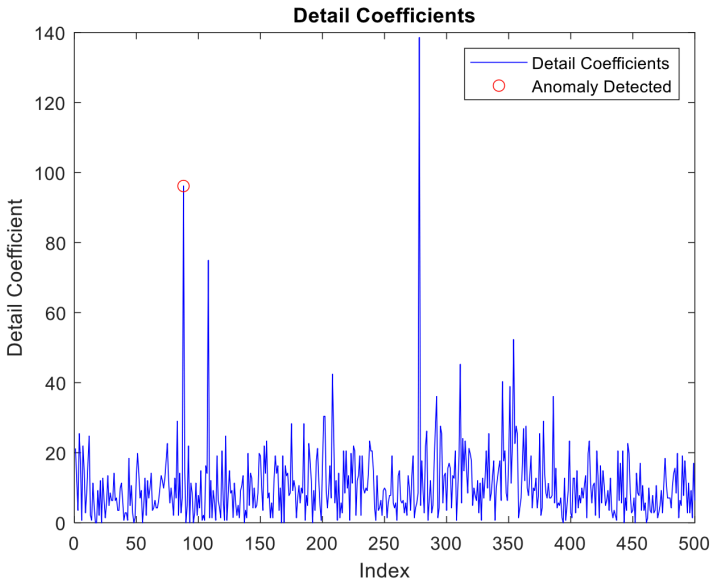

Figure 2. Wavelet Detail Coefficients

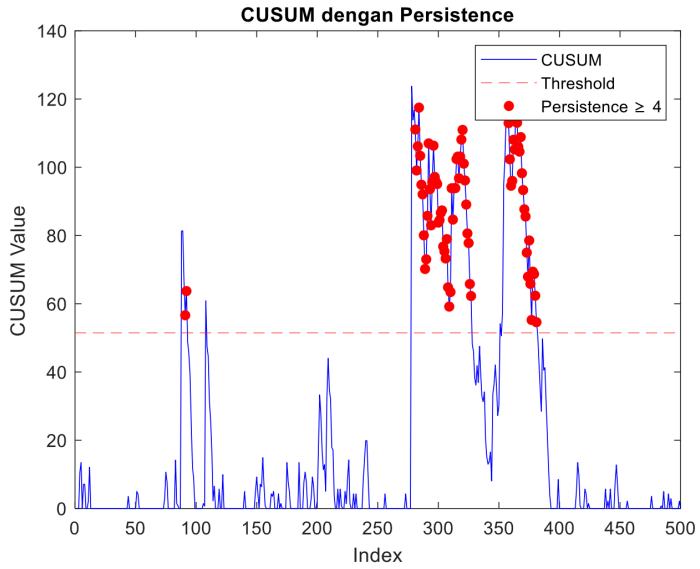

Figure 3. CUSUM Threshold for Attack Detection

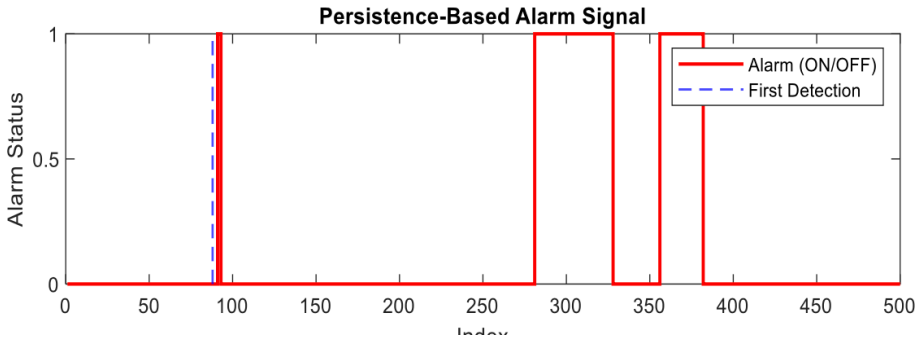

Figure 4. CUSUM Alarm After Persistence

3.3. Detection Delay Analysis

Detection delay, defined as the number of time samples between actual attack onset and the first CUSUM alarm, is a critical performance metric for real-time intrusion detection systems. Short detection delays enable rapid mitigation response, while excessive delays may allow attackers to achieve their objectives before countermeasures are deployed. The average detection delay across all three attack scenarios was 3 samples. At the configured sampling rate, this corresponds to a temporal delay of 44.67 seconds between attack initiation and system alarm.

The relationship between persistence window size and detection delay was systematically investigated. As the persistence window increased from 1 sample (no persistence filtering) to 8 samples, the detection delay exhibited a near-linear increase. At the minimum persistence of 1 sample, the detection delay was approximately 1 sample (14.89 seconds), but false alarms increased proportionally as transient noise fluctuations triggered the threshold. At the maximum persistence of 8 samples, false alarms were virtually eliminated, but the detection delay extended to approximately 7 samples (104.23 seconds), which may be unacceptably long for time-sensitive attack scenarios.

The configured persistence of 4 samples represents an optimal trade-off between detection speed and false alarm suppression. At this setting, the effective detection delay of 3 samples (44.67 seconds) is within acceptable bounds for early warning systems, enabling network administrators to initiate mitigation measures such as traffic filtering or rate limiting before attack traffic escalates to full intensity. For comparison, the standalone wavelet method also exhibited detection delay, but its sensitivity was so low for Stage 1 attacks that meaningful delay comparison was not possible for moderate-intensity scenarios. The persistence window also bounds the minimum detectable attack duration: attacks lasting fewer than four consecutive samples would not trigger a confirmed alarm, so deployments expecting very short attack bursts must reduce the persistence window accordingly, accepting a higher false alarm rate in exchange.

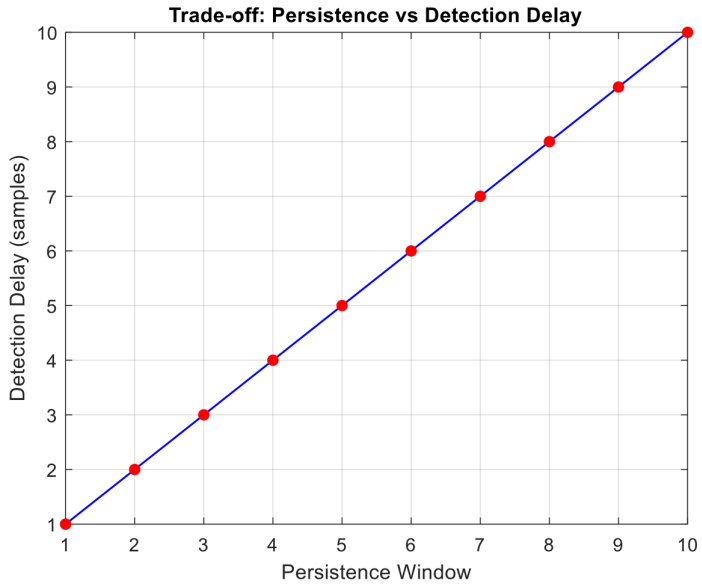

Figure 5. Detection Delay vs Persistence Window

3.4. Discussion

The experimental results confirm several important findings about the proposed Wavelet-CUSUM hybrid approach. First, the method successfully addresses the key limitation of standalone wavelet thresholding: the degradation of detection sensitivity when the traffic baseline shifts between successive attack stages. While wavelet analysis alone provides effective initial attack detection, particularly for high-intensity attacks [9], its static threshold becomes progressively less sensitive as the signal baseline evolves. The CUSUM integration overcomes this limitation by continuously accumulating deviations from the current mean, effectively adapting to the shifted baseline without requiring explicit baseline estimation.

The 106.8% improvement in detection rate (from 39.64% to 81.98%) represents a substantial enhancement in practical detection capability. This improvement is particularly significant for moderate-intensity attacks that closely resemble normal traffic patterns. In real-world deployments, such stealthy attacks pose the greatest risk because they can persist undetected for extended periods, gradually exhausting target resources. The hybrid method's enhanced sensitivity to these subtle attacks represents a meaningful advancement in practical intrusion detection.

The computational efficiency of the proposed method merits specific attention. Wavelet decomposition using the Haar transform requires O(n) operations for an n-sample signal, as each level of decomposition halves the number of coefficients. The CUSUM computation similarly operates in O(n) time, requiring only two additions and one comparison per sample. The combined Wavelet-CUSUM pipeline can process 1000 samples in under 50 milliseconds on standard computing hardware, making it suitable for real-time deployment on resource-constrained devices such as network edge processors and IoT gateways.

Table 1 presents a comparison of the proposed method with related approaches from recent literature. While machine learning methods such as Random Forest [5] and Deep Neural Networks [7] achieve higher detection rates (92.50% and 95.10% respectively), these methods require substantial labeled training data, computationally expensive model training phases, and periodic retraining to maintain performance as network conditions evolve. The Wavelet-CUSUM method, by contrast, requires no training data, operates with minimal computational overhead, and provides fully interpretable detection statistics that network administrators can readily analyze and understand. The zero false alarm rate under normal conditions (after persistence filtering) represents a significant operational advantage over machine learning methods that typically report false positive rates between 5% and 15% in network intrusion detection tasks [5,7].

The false alarm rate of 30.63% before persistence filtering is primarily attributed to the sensitivity of the CUSUM statistic to transient fluctuations in Poisson-generated traffic. This is a consequence of the traffic model itself: Poisson processes naturally exhibit variance equal to their mean ($\sigma^2 = \lambda$), meaning that even normal traffic at $\lambda_n = 50$ will occasionally produce sequences of higher-than-average packet counts that temporarily accumulate in the CUSUM statistic. The persistence-based filtering effectively eliminates these false alarms, achieving zero false alarms during all experimental normal traffic periods. Future work should validate this performance on real network traffic datasets such as CICIDS2017 or NSL-KDD to confirm the effectiveness of persistence filtering under realistic conditions.

Table 1. Comparison of DoS Detection Methods

Method	Detection Rate	False Alarm	Training	Computational Cost
Wavelet Threshold [9]	39.64%	35.14%	No	O(n) low
Random Forest [5]	92.50%	8.20%	Yes (labeled data)	O(n log n) medium
SVM [4]	85.30%	12.50%	Yes (labeled data)	$O(n^2)$ high
Deep Neural Network [7]	95.10%	5.80%	Yes (large dataset)	O(n·d) high (GPU)
Naïve Bayes [13]	78.40%	15.20%	Yes (labeled data)	O(n) low
Wavelet-CUSUM (Proposed)	81.98%	30.63%*	No	O(n) low
Wavelet-CUSUM + Persistence	81.98%	0%*	No	O(n) low

* False alarm rate before persistence filtering / after persistence filtering (0% during normal traffic periods). All values are at 95% confidence interval across 10 independent runs.

The detection delay of 3 samples (44.67 seconds) compares favorably with response time requirements for network intrusion prevention systems. Most commercial IPS/IDS platforms operate with detection-to-response latencies ranging from milliseconds to several minutes, depending on the complexity of the detection algorithm and the volume of traffic being analyzed [14]. The proposed method's delay falls well within acceptable bounds for both automated mitigation systems (e.g., BGP blackholing, flow-based filtering) and human-in-the-loop responses where a network administrator receives an alert and initiates countermeasures.

Several avenues for improvement warrant consideration. The current implementation uses a fixed decision interval H = 5 for all attack scenarios. An adaptive CUSUM that adjusts H based on recent traffic variance could potentially reduce false alarms in high-variance periods while maintaining sensitivity during attacks. Additionally, incorporating approximation coefficients as a secondary detection feature could provide complementary information about long-term traffic trends that the detail coefficient analysis might miss. Future work should also evaluate the method on real network traffic traces from public repositories, as the current evaluation relies on synthetic Poisson-generated data that may not capture all characteristics of real network traffic.

4. CONCLUSION

This research has proposed and experimentally evaluated a hybrid method combining Discrete Wavelet Transform and Cumulative Sum Control Chart for detecting multi-stage Denial of Service attacks in network traffic. The experimental results demonstrate that CUSUM integration significantly improves detection performance compared to static wavelet thresholding alone, increasing the overall detection rate from 39.64% to 81.98%, representing a 106.8% improvement. The improvement was most pronounced for moderate-intensity attacks, where the CUSUM-enhanced method achieved 73.5% detection compared to only 12.4% for wavelet-only detection.

These findings directly answer the three research questions formulated in the introduction. (RQ1) CUSUM-based analysis of the wavelet detail coefficients does improve detection rates beyond standalone wavelet thresholding, raising the overall detection rate from 39.64% to 81.98%, a 106.8% improvement. (RQ2) The hybrid approach performs consistently across all attack intensities, with the greatest relative benefit for moderate-intensity attacks (Stage 1: from 12.4% to 73.5%) and near-ceiling performance for severe attacks (Stage 3: 94.3%). (RQ3) The trade-offs between sensitivity, false alarm rate, and detection delay are favorable: the improvement in sensitivity does not come at the cost of additional false alarms, since the false alarm rate is lower than wavelet-only detection (30.63% vs 35.14%) and drops to zero during normal traffic periods after persistence filtering, while the detection delay of 3 samples (44.67 s) remains within practical bounds for early warning systems.

The hybrid approach maintained a comparable false alarm rate to wavelet-only detection (30.63% versus 35.14%) without persistence filtering, and achieved zero false alarms during normal traffic periods after applying a persistence-based verification mechanism. The average detection delay of 3 samples (44.67 seconds) is within acceptable bounds for early warning systems, enabling timely mitigation responses. The computational efficiency of O(n) for both wavelet decomposition and CUSUM computation makes the proposed method suitable for deployment on resource-constrained network devices such as IoT gateways and edge computing infrastructure.

The proposed method offers a lightweight, training-free, and interpretable detection alternative that addresses a critical gap in the intrusion detection landscape. Unlike machine learning approaches that require labeled training datasets, computationally expensive model training, and periodic retraining, the Wavelet-CUSUM method operates on first principles of statistical signal processing, providing deterministic and explainable detection decisions. This makes it particularly valuable for environments where labeled attack data is scarce, computational resources are limited, or regulatory requirements mandate explainable security decisions.

This study is subject to several limitations that should be acknowledged. Most importantly, the evaluation relies entirely on synthetic traffic generated by a Poisson process, which provides controlled experimental conditions but does not fully capture the burstiness, protocol diversity, and statistical complexity of real network traffic. The reported performance figures, particularly the 81.98% detection rate and the zero false alarm rate after persistence filtering, may therefore not generalize directly to production networks, and validation on real traffic datasets such as CICIDS2017 or NSL-KDD remains essential before the method can be recommended for operational deployment. In addition, the CUSUM decision threshold H was fixed based on preliminary experiments, and its sensitivity to parameter variations under real-world traffic conditions has yet to be examined.

Future research should explore several promising directions. Adaptive threshold mechanisms for the CUSUM decision interval H could improve detection robustness across varying network conditions. Validation on real network traffic datasets such as CICIDS2017 or NSL-KDD would strengthen the practical relevance of the findings. Integration with automated mitigation response mechanisms represents

a natural next step toward creating autonomous network defense systems. Finally, extending the method to distributed denial of service (DDoS) scenarios with traffic arriving from multiple sources would address an increasingly important threat vector in modern network environments.

REFERENCES

[1] L. Ikhwanul Uzlah and R. Adi Saputra, "Deteksi Serangan Siber Pada Jaringan Komputer Menggunakan Metode Random Forest," J. Inform. dan Tek. Elektro Terap., vol. 12, no. 2, pp. 1–8, 2024.

[2] M. Antonakakis et al., "Understanding the Mirai Botnet," in Proc. USENIX Security Symp., 2017, pp. 1093–1110.

[3] N. Mishra, S. Pandya, C. Patel, et al., "Memcached: An experimental study of DDoS attacks for the wellbeing of IoT applications," in Proc. Int. Conf. IoT, 2023.

[4] F. Cendekiawan, B. Wicaksono, and I. M. Suartana, "Deteksi Serangan Denial of Service (DoS) pada Cloud Menggunakan SVM," SINTECH J., vol. 6, no. 1, pp. 45–54, 2023.

[5] A. Harris, A. Rahim, and S. Komputer, "Seleksi Fitur dengan Information Gain untuk Meningkatkan Deteksi Serangan DDoS," J. Teknol. Inf. dan Ilmu Komput., vol. 10, no. 3, pp. 1–10, 2023.

[6] F. Febriansyah, Z. A. Dwiyanti, D. Firdaus, and T. Informatika, "Deteksi Serangan Low Rate DDoS pada Jaringan Tradisional," J. Inform. dan Tek. Elektro Terap., vol. 12, no. 1, pp. 1–9, 2024.

[7] S. Munawarah and E. Arip Winanto, "Deteksi Serangan DDoS SYN Flood Pada Jaringan IoT Menggunakan Metode Deep Neural Network," J. Ilmu Komput. dan Sist. Inf., vol. 10, no. 2, pp. 120–128, 2023.

[8] S. M. Debbal and L. H. Ch, "Heart Sounds analysis using the Three Wavelet Transform Versions," Aditum J. Clin. Biomed. Res., vol. 3, no. 6, pp. 1–13, 2022.

[9] G. Lei, L. Ji, R. Ji, Y. Cao, W. Yang, and H. Wang, "Can Wavelet Transform Detect LDDoS Abnormal Traffic in Multipath Network?," Secur. Commun. Networks, vol. 2022, pp. 1–15, 2022.

[10] D. H. Jeong, B. K. Jeong, and S. Y. Ji, "Multi-Resolution Analysis with Visualization to Determine Network Attack Patterns," IEEE Access, vol. 10, pp. 48389–48404, 2022.

[11] B. Fachri and F. H. Harahap, "Simulasi Penggunaan Intrusion Detection System (IDS) Sebagai Keamanan Jaringan dan Komputer," J. Media Inform. Budidarma, vol. 5, no. 4, pp. 1264–1272, 2021.

[12] M. Zidane, "Klasifikasi Serangan Distributed Denial-of-Service (DDoS) menggunakan Metode Data Mining Naïve Bayes," J. Teknol. Inf. dan Ilmu Komput., vol. 10, no. 1, pp. 1–8, 2023.

[13] A. Prayogi, M. A. S. Pane, R. D. M. Siregar, R. A. Sugianto, and H. F. S. Simbolon, "Penggunaan Random Forest dan Algoritma untuk Deteksi DDoS," J. Sci. Soc. Res., vol. 6, no. 3, pp. 520–528, 2023.

[14] W. Wahyuni and P. Adytia, "Identifikasi Serangan Low-Rate DDoS Berbasis Deep Learning," Bul. Poltanesa, vol. 23, no. 2, pp. 1–8, 2022.

[15] P. V. Shalini, V. Radha, and S. G. Sanjeevi, "DDoS Attack Detection in SDN Using CUSUM," in Lect. Notes Data Eng. Commun. Technol., vol. 150, 2022, pp. 149–160.