# *A Hybrid Deep Learning Framework For Early Detection Of Distributed Denial-Of-Service Attacks In Communication Networks*

Rahul Vijay Kotawadekar[1*], Dr. Suhasini Vijaykumar[2], Bhushan S. Deore[3], Amit S. Tiwari[4], Jitendra P. Sonawane[5], Monu[6], Kyaw Myo Tun[7]

[1*]Research Scholar, Department of Computer Applications, Bharati Vidyapeeth's Institute of Management & Information Technology, Navi Mumbai, India 400614, Affiliated to University of Mumbai, Mail id: rahulkotawadekar@hotmail.com ORCID ID - 0009-0002-1923-6139
[2]Professor and Principal, Department of Computer Applications, Bharati Vidyapeeth's Institute of Management & Information Technology, Navi Mumbai, India, 400614, Affiliated to the University of Mumbai. Mail id: suhasini.kottur12@gmail.com
[3]Assistant Professor, Department of Electronics and Communication Engineering, Ramrao Adik Institute of Technology, D. Y. Patil Deemed to be University, Navi Mumbai, India 400706. Email ID: bhushan.deore@dypatil.edu ,ORCID ID: 0000-0003-3602-711X
[4]Assistant Professor, Department of Electronics and Computer Science Engineering, Shah and Anchor Kutchhi Engineering College, Mumbai, India 400004. Email ID: amit.tiwari@sakec.ac.in , ORCID ID: 0009-0003-2014-7704
[5]Assistant Professor, Department of Electronics and Communication Engineering, Ramrao Adik Institute of Technology, D.Y. Patil Deemed to be University, Navi Mumbai, Mumbai 400706. Email ID: Jitendra.sonawane@dypatil.edu, ORCID ID: 0000-0002-0240-2332
[6]Assistant Professor, School of Information Science, Department of Computer Science & Engineering, Presidency University, Bengaluru, India 560119, Email Id: monujakhar012@gmail.com, ORCID ID: 0009-0007-1304-0844
[7]Masters in Information Technology INTI International University, Malaysia ORCID ID:0009-0009-9653-734X Email ID: i25033420@student.newinti.edu.my

***Abstract***
DDoS attacks can be discussed as a significant cybersecurity threat because, despite their quick activation, they can turn network resources to overflow within a few seconds. Most current detection studies however have high accuracy when the datasets are highly imbalanced, which is not realistic in the operation demands of early warning. The proposed study suggests a hybrid deep learning model that would utilize Convolutional Neural Networks (CNN) and Long Short-Term Memory (LSTM) networks to enhance the reliability of the classification process and the ability to predict attacks by time. Experiments were performed with CIC-DDoS2019 dataset and 28 selected flow level features. A strict sliding window strategy (W = 60, S = 10) was used to convert network flows into sequential samples, for which windows were considered as attacks only whenever all the 60 flows were malicious. Two models were tested, CNN model alone and the proposed CNN - LSTM model. Results show that CNN--LSTM had a better performance at window level, which achieved ROC-AUC=0.982, PR-AUC=0.962, Macro-F1=0.976 than CNN-only (ROC-AUC=0.845, PR-AUC=0.809, Macro-F1=0.786). Under natural test conditions (97.8% attack windows), CNN--LSTM achieves an accuracy of 0.993 and Macro-F1 = 0.924. However, row-truth episode-based evaluation resulted in the miss rate of 0.746 for both the models, making it clear that it is difficult to detect attacks at their earliest onset. Overall, the findings confirm that CNN-LSTM improves performance in classification and strict episode-based evaluation results show that true onset-level early detection is still a challenging problem.

***Keywords:*** Distributed Denial-of-Service (DDoS) Detection, Hybrid Deep Learning (CNN–LSTM), CIC-DdoS2019 Dataset, Sliding Window Traffic Modeling, Episode-Based Early Detection.

## *1. Introduction*

Distributed Denial of Service attacks (DDoS) have been one of the most persistent and disruptive threats to modern communication networks, cloud infrastructures and Internet of Things (IoT) environments [1]. By overloading the targeted services with huge volumes of malicious traffic, the DDoS attacks can result in service unavailability, financial losses and severe degradation of quality of service, especially in latency sensitive and mission critical systems [2]. The growing use of heterogeneous networked systems such as IoT, software-defined networks (SDN), cyber-physical systems and vehicular ad hoc networks (VANETs), has further widened the attack surface hence rendering traditional defence mechanisms increasingly inadequate [3].

Early research has been done on DDoS detection that emphasized rule-based systems, statistical threshold and signature-based intrusion detection systems, but these methods have difficulty adapting with the demand of evolving patterns of attacks, encrypted traffic and higher speed networks [4]. In response, the techniques of machine learning (ML) and deep learning (DL) have attracted a great deal of attention, owing to their capacity to learn from the data without explicit formulation of rules for the complex traffic patterns [5]. Recent research has shown the power of deep neural networks for identifying DDoS attacks in Internet of Things (IoT) environments, where deep learning models that combine elements of deep learning networks and machine learning have been shown to have increased accuracy and robustness under constrained network conditions [6]. Deep learning techniques have also been successfully applied to vehicular ad hoc networks (VANETs) in order to both detect and mitigate DDoS attacks in highly dynamic network topologies [7]. In cloud computing environments, deep learning-based DDoS detection systems have been proposed to cope with the large-scale traffic volume and distributed attack sources compared to the traditional methods [9]. Similarly, deep learning techniques have been applied for software-defined networking (SDN) architectures in order to enhance attack detection performance by taking advantage of centralized control and worldwide traffic visibility.

Despite these gains, there are several important challenges to be resolved. First, many existing studies mainly consider the window-level classification performance, and the classification accuracy, precision, or area-under-curve values are often extremely high, which may fail to reflect the practical performance [10]. Such metrics can be misleading in highly imbalanced datasets where attack data samples are dominating benign traffic or where detection is assessed after attack data has totally manifested [11]. Second, most models are optimized to attack identification instead of early detection, which is very important to enable timely mitigation before network resources are exhausted [12]. Third, most of the detection methods are based on static characteristics or simple model, which cannot reflect the temporal dynamic changes of traffic flow, so they are not robust for low-rate, slow-starting, or reflection DDoS attacks [13].

As a solution to these constraints, recent studies have been done on hybrid deep learning architectures that fuse convolutional neural networks (CNNs) with recurrent networks, e.g. long short-term memory (LSTM) networks. CNNs are good in capturing the spatial and local temporal patterns of the traffic features, whereas LSTMs are good in modeling long-term dependencies and the sequential behavior, and thus the combination of CNN and LSTM is useful in the context of time evolving network attacks [14]. Much of hybrid methodology, however, continues to measure performance in traditional classification terms without specifically measuring detection delay or episode-level behavior, which creates a disjuncture between the reported performance and practice in application.

This work is inspired by the fact that realistic operationally meaningful DDoS detection frameworks are required that focus more on the early detection as opposed to the post-hoc classification. Instead of focussing only on the prediction accuracy at a window level, this work investigates a detection performance metric at the episode level (how fast after

the beginning of an attack, it can be detected, how many attack episodes can be missed completely), to measure the detection performance. Such an evaluation paradigm is closer to the practical deployment scenarios where the main goal is to detect the attack within seconds and to trigger mitigation mechanisms before the service degradation takes place.

The aim of this research work is to design and evaluate a hybrid CNN-LSTM model for early DDoS identification at the communication networks based on flow-based traffic features. The proposed approach is evaluated through representative DDoS attack types including SYN flood, UDP flood and LDAP-based reflective attacks based on a realistic benchmark dataset. The paper directly compares hybrid CNNLSTM model with CNN only baseline to determine the role of temporal modelling in early detection. Although the framework has been confirmed in several types of attacks, there is no explicit mention on encrypted payload inspection, real-time preventative plans, and adversarial evasion methods, which are not the focus of the current study.

The importance of this study is that it moves away from reporting inflated performance towards realistic early detection analysis. By getting episode-based metrics such as in seconds detection delay, in constrained time budgets as detection rate, missed attack episodes, this work gives a more trustworthy and deployment oriented assessment of DDoS detection performance. Furthermore, the comparison of CNN-only and CNN-LSTM architectures provides useful information about the role of temporal learning in improving the robustness and lowering the detection latency, especially for attacks with gradual building of traffic.

The primary objectives of this research are as follows:

- To formulate a hybrid CNN-LSTM deep learning model that can be used to detect both spatial and temporal patterns in network traffic for an effective DDoS attack detection.
- To assess the detection performance in terms of the early detection measures at the episode level rather than the accuracy-based measures, paying the attention to the detection delay and response speed.
- To compare the proposed CNN-LSTM hybrid model with a CNN-only baseline model to quantify the benefits of temporal sequence learning.
- To analyse detection behaviors for different types of DDoS attacks under realistic time-budget constraints (e.g. detection within 1s, 5s, and 10s).

The contribution of this work to the existing literature on deep learning-based DDoS detection is by fulfilling these aims and focusing on their relevance in practice, readability, and the effectiveness of a timely response. The results show that hybrid temporal models can provide timely detection with stable performance over attack types, which is a promising line for network security systems in the future.

## *2. Literature Review*

Recent years have seen a vast amount of research efforts towards improving the detection and mitigation of Distributed Denial-of-Service (DDoS) attacks through machine learning and deep learning techniques, especially in the emerging and heterogeneous network environment. Early efforts have been invested in adapting conventional machine learning models for IoT networks, and it was shown that it is feasible to use supervised learning to obtain acceptable detection accuracy in controlled environments [15]. Nevertheless, these methods tended to suffer performance decline in case of dynamic traffic and in massive attack conditions. To overcome the limitations of single model learning, attention based and ensemble deep learning techniques have been introduced. A self-attention enabled weighted ensemble convolutional neural network was proposed to improve the feature representation and classification accuracy in the DDoS traffic [16]. While this

approach provided a good classification performance, it mainly focused on the offline detection and did not explicitly consider the early detection or real-time constraints.

In the area of software-defined networking and aerial network architectures, ensemble learning in combination with honeypot mechanisms have been researched for DDoS detection and mitigation [17]. Such centralized architectures showed a better effectiveness of mitigation but gave rise to a more complex network system with limitations to scalability in high-speed or large-scale network deployments. Deep learning-based DDoS detecting has been also studied in intelligent transportation and high-availability network systems. A deep neural framework was proposed to defend intelligent transport infrastructure against large-scale DDoS attacks, in which the deep learning model's ability to handle large traffic levels is confirmed [18]. However, the evaluation concerned predominantly the detection accuracy without taking into account the detection latency and temporal attack evolution.

Temporal modeling by recurrent neural networks has become popular for modeling sequential behavior of traffic. A DDoS detection and defense system based on the Long Short-Term Memory network for public clouds was developed revealing that sequential learning achieves higher accuracy in the detection of DDoS attacks compared to static classifiers [19]. Despite these benefits, the analysis was still flow based and did not quantify the delays in early detection or the performance at the episode level. Feature optimization has been found to be an important factor in enhancing the precision of the detection process, especially for low-rate DDoS attacks. An optimised feature selection strategy with a deep learning approach was suggested for the improved detection of stealthy attacks [20]. The use of large-scale preprocessing and feature engineering, however, became a cause of concern in as far as real-time applicability is concerned.

Beyond the traditional network security application, deep learning model has been applied to behavioral anomaly detection using DDoS related traffic features [21]. While this proved the versatility of DDoS flow characteristics, the study was not focused on a network-level early attack detection or operational deployment cases. Supervised machine learning methods have kept improving in a step-wise manner in improving DDoS detection [22]. Nevertheless, these studies were often based on static datasets and had no evaluation frameworks based on time or episodes.

There is an increase in the use of deep learning architectures that consist of both a convolutional and recurrent part. A hybrid model that combined CNN and RNN layers was proposed for DoS/DDoS detection in software defined networks, which gave an improved detection capability [23]. Despite its effectiveness, the evaluation was still window-based and did not evaluate the detection latency at the attack-episode level. Data preprocessing and traffic feature engineering have also been found to play an important role in the detection performance. Improved data processing pipelines were suggested to improve the accuracy of DDoS detection based on machine learning [24]. However, such approaches were usually focused on the quality of features rather than temporal detection behavior.

More advanced combinations of optimization and swarm intelligence have been implemented into the deep learning models for IoT-based DDoS detection which gave high detection rates with the increasing computational complexity [25]. Similarly, feature pruning in combination with optimized deep learning models improved the detection precision in IoT environments albeit the feasibility of real-time detection was a challenge [26]. Domain-specific DDoS detection has been investigated for IoT-based banking monitoring systems where the traditional machine learning based detection models proved effective, but were not able to adapt to changing patterns of attacks [27]. Addressing data imbalance A deep learning framework to enhance minority class detection in imbalanced DDoS datasets was proposed, even though the evaluation focused

mainly on the accuracy metrics [28]. Finally, hybrid machine learning approaches of several algorithms have been proposed to improve robustness in various scenarios of DDoS attacks [29]. Although these frameworks presented good outcomes, they failed to specifically compare the time latency of early detection or episode-wise performance.
The reviewed literature shows a great deal of progress in the detection of DDoS attacks with the application of machine learning and deep learning techniques. However, most of the existing studies focus on the classification accuracy and the window-level evaluation with little attention to the early detection, the episode-level analysis, and the detection delay. These gaps suggest the need for hybrid temporal models that are evaluated by realistic, episode-based early detection metrics and are the motivation for the approach taken in this study.

## *3. Methodology*

### *3.1 Research Design*

This research is an experimental study with a quantitative research design to investigate a hybrid deep learning framework for the early detection of Distributed Denial-of-Service (DDoS) attacks in communication networks. The problem is formulated as a supervised binary classification problem, where the goal is to classify time ordered network traffic as benign (0) or attack (1). In addition to traditional methods of evaluating classification, the study includes an episode-based early detection protocol that measures how quickly a model detects an attack after it has started. This makes the evaluation consistent with operational requirements for DDoS defense, where it is more important to detect as quickly as possible rather than to be accurate alone when there is a severe class imbalance (see Fig. 1).

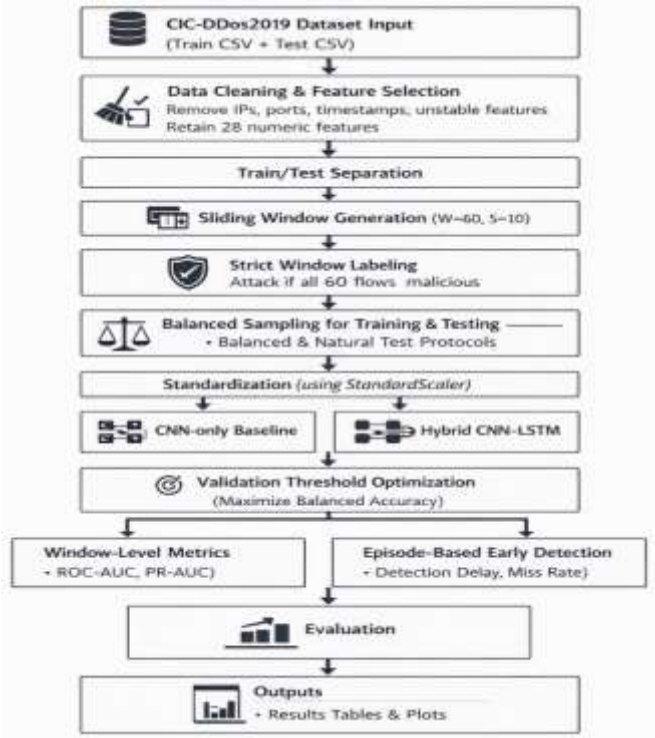



***Figure 1. Methodology Flowchart of the Proposed Hybrid CNN–LSTM Framework for Early DDoS Detection***

Fig. 1 presents the overall experimental pipeline for this study, which starts with the input of data from CIC-DDoS2019 after preprocessing, the generation of a strict sliding window and its standardization. It also shows CNN-only and hybrid CNN-LSTM model training is compared and validation-based threshold optimization is performed. Finally, the framework scores performance in terms of both window-level classification metrics, and episode-based early detection metrics, which is presented to the user in the form of final results tables and plots.

The research is comparative, and tests a proposed CNN-LSTM model against a CNN only baseline. This allows us to systematically evaluate the temporal sequence modeling (through LSTM) to better performance and stability detection than using convolutional feature extraction. All experiments are done offline in a controlled fashion with an benchmark data set, with results presented in terms of both classical classification metric and time early detection indicators.

### *3.2 Data Collection Methods*

The dataset considered in this research study is based on the CIC-DDoS2019 benchmark dataset developed by the Canadian Institute for Cybersecurity (CIC) [30]. CIC-DDoS2019 contains realistic DDoS traffic captured in network environments and processed by CICFlowMeter that generates flow-level statistical features.

Traffic is given in CSV format and includes benign flows as well as several categories of DDoS attacks. A subset of attack families was chosen in order to have diversity and at the same time be computationally feasible; they included the most senior DDoS behaviors, such as reflection/amplification attacks, volumetric flooding, and TCP resource exhaustion. Files were gathered from training day and testing day folders to ensure the temporal separation of training and evaluation scenarios. The training data consisted of DrDoS_DNS.csv, DrDoS_NTP.csv, DrDoS_UDP.csv, and Syn.csv and the test data consisted of LDAP.csv, UDP.csv, and Syn.csv. These files offer variation across the types of protocols and attack dynamics of relevance to early detection analysis.

### *3.3 Population and Sampling Strategy*

The population is represented by CIC-DDoS2019 flow records of benign communication and DDoS attack scenarios. Each record is associated with a bi-directional aggregated flow that has temporal statistics (e.g. inter-arrival times), packet-level distributions (e.g. packet length statistics), and protocol counters (e.g. TCP flags). CIC data sets are very large and it's not practical or necessary to train them in full. Therefore, sample collection was done at window level after preprocessing and the sequence construction. This choice is of methodological importance because the model input is not the individual flow, but a sequence of flows. The dataset was cleaned and merged separately into train and test dataset. After the preprocessing, the combined training data included approximately 11 million flows and combined testing data included approximately 10 million flows.

Given the preponderance of attack traffic in CIC-DDoS2019, class imbalance is high. Instead of balancing to a prescribed benign/attack ratio at the flow level (which may distort the temporal structure) balancing was the strategy at the window level, and strict window labeling of Section 3.5. Specifically, an equal amount of benign and attack windows were sampled for training, in an effort to avoid trivial attack-dominant decision boundaries. This gave an equal dataset of 33,988 training data (50: benign, 50: attack). To make an evaluation, both balanced and naturally imbalanced test windows were kept to make a good comparison and deployment-oriented evaluation.

### *3.4 Data Preprocessing and Feature Engineering*

Raw CICFlowMeter outputs contain fields that can cause model bias, instability and leakage. Preprocessing was done prior to the construction of the window and training of the models.

The following categories were removed:

- Identity and Leakage Prone Fields: Flow ID, Source IP, Destination IP, ports and timestamps, so that one cannot memorize endpoints.
- Unstable rate features such as Flow Bytes/s and Flow Packets/s that can lead to extreme values as a result of near-zero flow duration.
- Redundant/constant attributes, including attributes related to bulk and non-informative columns.

A final set of 28 numeric features was kept, which reflects temporal behavior, packet statistics and protocol characteristics. These are duration features, IAT metrics, packet length distributions, directional packet features and flag counters.

Feature scaling has been done using Z score standardization. A StandardScaler was only fit on training windows and was applied to both the training and test windows using the same set of fitted parameters to avoid leakage on the test data.

### *3.5 Sliding Window Generation and Sequence Modeling*

Early DDoS detection requires modeling the evolution of traffic over time instead of the independent sample of flows. Flow records were converted into fixed length sequences based on a sliding window mechanism. W = 60 consecutive flows are in each window with a stride of S = 10 giving rise to intersecting sequences and maintaining continuity in time. This configuration has enough temporal context, but it is computationally feasible.

To ensure that positive predictions were associated with sustained rather than short-term attack behaviour, a very strict labelling rule was applied:

- A window is labeled Attack (1) only if all 60 flows in the window are malicious.
- Otherwise, it is labeled Benign (0).

This results in a high-confidence definition of attack at the window level and brings the learning objective in line with realistic alerting requirements (i.e. alarm should be triggered during clearly established attack periods). After windowing the dataset is represented as:

$$X \in \mathbb{R}^{N \times 60 \times 28},$$

where $N$is the number of windows, 60 is the temporal length, and 28 is the feature dimension.

A balanced training window set was constructed by sampling equally the number of benign and attack windows. For testing, both (i) balanced test windows and (ii) natural (deployment-like) windows were used for testing the model behavior under different class distribution.

### *3.6 Data Analysis Techniques*

Two deep learning models were implemented:

- CNN-only baseline: a 1D CNN extracting local feature patterns inside windows catching short-term changes in packet statistics, e.g. sudden changes of packet statistics.
- Hybrid CNNLSTM (proposed): CNN layers are used to obtain the discriminative representations, and then LSTM layer is used to predict time dependency over the sequence of windows. This helps in the identification of changing patterns of attacks and enhances temporal stability.

Both the models were trained with Adam optimizer and binary cross-entropy loss. Using stratified sampling, training was divided into 80% training / 20% validation. To minimize residual imbalance effects without requiring implausible perfection, class weighting was

carried out which had a limit of extreme benign weights. To stabilize convergence and minimize overfitting, it was done by early stopping and learning-rate scheduling.
Rather than setting a threshold to 0.5, balanced accuracy on the validation set was used to tune model specific decision thresholds, which were then fixed for all evaluations. This averts the optimistic bias and facilitates the fair comparison of models under imbalance.
Evaluation metrics.
- Window level classification: confusion matrix, precision/recall/F1, ROC-AUC, PR-AUC, balanced accuracy and macro-F1.
- Early detection by the episodes: the traffic was grouped by Destination IP and divided into attack episodes.

Two-episode definitions were evaluated:
- Window-truth episodes: consecutive attack-labeled windows (consistent with training labels).
- Row-truth episodes: consecutive evil flows (stronger and more realistic).

For each episode, detection coverage and detection delay were calculated including; episode miss rate, detection delay in seconds, median/mean/tail delay, and detection rate within time budgets (1s, 5s, 10s). This multi-level design ensures that performance gains are indicative of significant changes in early detection as opposed to an effect of imbalance or lax labelling.

### *3.7 Ethical Considerations*

This research uses benchmarking from a publicly available dataset and has no human subjects or private organizational logs. Ethical principles in cybersecurity were adhered to: strict use of the dataset for defensive research, no malicious implementation, transparent reporting of the results, and acknowledging the source of the dataset. The methodology focuses on a focus on realistic evaluation (episode-based detection) to prevent overstating of deployment readiness based on overstated window-level accuracy.

## *4. Results*

This section describes the experimental results of the proposed hybrid CNN- LSTM model for early DDoS detection with the use of CIC-DDoS2019 dataset. Two levels of evaluation were considered as complimentary:
- Window-level binary classification performance.
- Episode-based early detection performance.

While window-level metrics are used to get a first impression of discrimination capability, the episode-based evaluation is focused on as real-world DDoS mitigation systems require detection in seconds after the attack onset and not accuracy on high-imbalanced datasets. Hybrid CNNLSTM model is contrasted to CNN only baseline in terms of the contribution of temporal sequence modeling to the detection reliability and early response.

### *4.1 Window-Level Classification Performance (Binary Detection)*

Binary classification of windows was performed on windows of W = 60 flows and stride of S = 10 and the resultant overlapping sequences maintains sequential continuity. Strict labeling was used, where a window was only labeled as an attack when all 60 flows were malicious and positive predictions indicated sustained attack behavior not a short term contamination. The test was done in two complementary test environments: balanced windows (equal benchmark and attack samples) to compare unbiased and natural windows (respectively, 97.8% attack windows as the original dataset distribution). To prevent arbitrary rules for decision making, in order to tune model specific thresholds, a maximum balanced accuracy was obtained for the validation set and these thresholds

were fixed for all experiments. The ideal value was 0.9 for CNN-LSTM and approximately 0.55 for CNN-only. On balanced testing, CNN-LSTM had about 97.6% balanced accuracy and macro-F1, which is much higher than CNN-only (=78.9%), primarily because of decreased false negatives. Both models were found to be highly accurate overall in natural testing (with the dominance of attacks) but CNN-LSTM exhibited greater macro-F1 whereas CNN-only quickly worsened, which attests to the fact that temporal modeling enhances robustness over imbalance artifacts. These findings provide motivation for the next episode-based early detection evaluation presented.

### *4.2 Episode-Based Early Detection Performance (Seconds-Level Evaluation)*

In order to evaluate the early detection capability in realistic deployment conditions, an episode-based evaluation framework was used. Traffic was classified by Destination IP and put in chronological order. Continuous periods of malicious activity were considered attack episodes and detection was considered episode-wise. For each episode, sliding windows were generated taking the same configuration as training. The earliest window predicted as malicious was used to calculate detection delay, and reported in both window progression and seconds (difference between episode start and detected window end).

Two definitions of the episode were considered:

- Window-truth episodes, formed from consecutive attack-labeled windows using the strict training labeling rule.
- Row-truth episodes, formed directly from contiguous malicious flows, independent of window boundaries.

The row-truth definition represents the most realistic and challenging evaluation scenario.

***Table 1: Episode-Based Early Detection Performance (Row-Truth Episodes)***

| Model | Total Episodes | Detected Episodes | Missed Episodes | Miss Rate | Median Delay (s) | Mean Delay (s) |
|---|---|---|---|---|---|---|
| CNN–LSTM | 59 | 15 | 44 | 0.746 | 0.015 | 111.05 |
| CNN-only | 59 | 15 | 44 | 0.746 | 0.016 | 111.37 |

Table 1 gives results on early detection when using the stricter definition of row-truth episode. Both CNN-LSTM and CNN-only were able to detect 15 out of 59 episodes, which means a high miss rate of 74.6%, indicating that the onset of attacks can hardly be distinguished from benign traffic. The median delay is close to zero seconds, that is detected episodes are often found immediately. However, the mean delay is greater than 110 seconds showing a heavy tailed delay distribution due to a small number of very late detections. Unlike window-truth episodes, row-truth episodes are the true flow-level beginning episodes of attacks, which is more realistic and serious for the deployment evaluation purpose.

### *4.3 Detection Performance Under Practical Time Budgets*

In operational DDoS defense systems, detection must take place in tight time limits. Therefore, episode detection success rates were measured in 1s, 5s and 10s time budgets using the row-truth definition.

***Table 2: Episode Detection Rate Within Time Budgets (Row-Truth Episodes)***

| Model | ≤ 1 s Detection (%) | ≤ 5 s Detection (%) | ≤ 10 s Detection (%) |
|---|---|---|---|
| **CNN–LSTM** | 25.4 | 25.4 | 25.4 |
| **CNN-only** | 25.4 | 25.4 | 25.4 |

The results in table 2 indicate that both models were able to detect at the same rate of 25.4% within 1 second and this rate did not change for time budgets of 5 s and 10 s. It means that there is a close binary detection trend of row-truth assessment: the episodes are either detected almost instantly or not detected at all despite a prolonged observation. The fact that longer budgets of time fail to improve indicates that often the early-stage malicious traffic is statistically similar to benign flows. This behavior is mainly influenced by strict episode boundaries and a strict windows labelling, which stresses the need to improve a sensitive early onset to prevent longer observation windows.

### *4.4 Graphical Analysis of Early Detection Trends*

To offer an intuitive understanding of early detection behavior in addition to tabular results, two visual analyses were performed with episode-level evaluation metrics based on the test dataset.

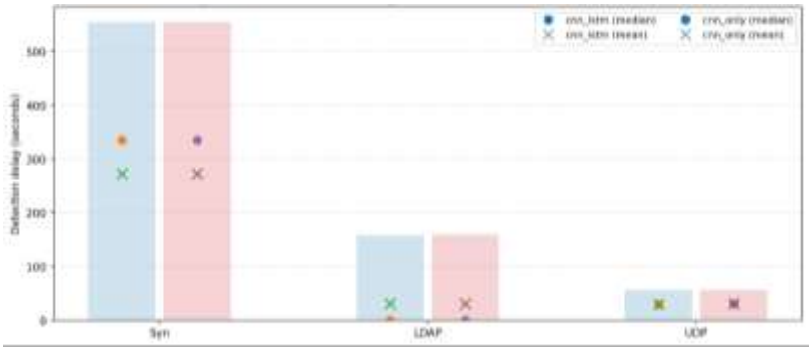



***Figure 2: Episode-Based Detection Delay Distribution***

**Figure 2** summarizes episode-based detection delay using median, mean, and 95th percentile tail delay. SYN and LDAP attacks exhibit near-zero median delays, reflecting strong and distinctive signatures. UDP attacks show higher delays, as early traffic resembles benign bursts. The CNN-LSTM shows more stable behavior of tails, which means controlled worst case delay.

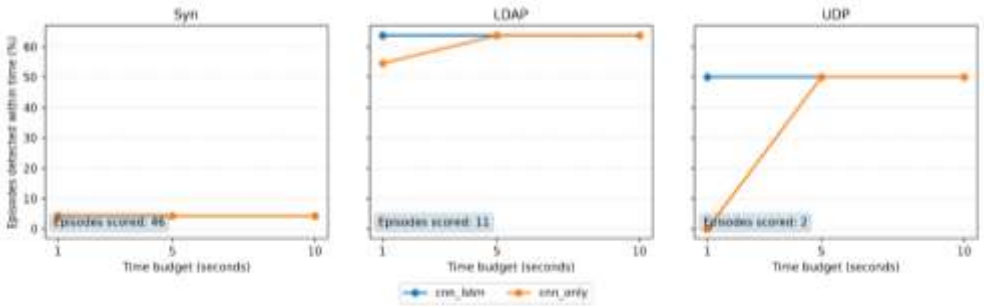



***Figure 3: Detection Rate vs. Time Budget***

**Figure 3** illustrates detection rate versus time budget. For SYN and LDAP attacks, there is a constant detection rate regardless of the budget, so either detection is either early or it is not. UDP attacks have low detection rates with little improvement over time. Across all attacks, both the models have similar timing behavior, but the CNN- LSTM identifies more difficult episodes on the whole.

Overall, both models have good performance in terms of individual windows, however, window-level metric alone is not enough to learn about the early detection capability. The hybrid CNN--LSTM model proves to be more temporally stable and robust, which supports its applicability for real-time DDoS detection systems where early warning and controlled detection delay are of great importance.

## *5. Discussion*

This research sought to go beyond traditional evaluation of DDoS detection models that focuses on accuracy by focusing on early detection behavior and employing realistic operational conditions. Prior work has focused on the fact that accuracy-based evaluation can be misleading if intrusion detection datasets are highly imbalanced [12]. The results of this research give important insights into how deep learning models work when measured at the window level, as well as at the episode level where detection delay and missed attacks become critical.

At the window level, the CNN-only and the CNN-LSTM hybrid models performed well in binary classification. The confusion matrix analysis using balanced test conditions revealed that both architectures are particularly good in distinguishing between benign and attack windows with high true positive and a significantly low number of false negativities. It is worth noting that the CNN-LSTM showed lower false negatives than the CNN-only baseline, which means that it is more sensitive to the behavior of the attackers when the distribution of classes is managed. High ROC-AUC and PR-AUC values are a further indication that the models learn meaningful traffic representations. However, these results also support a known limitation - in highly imbalanced circumstances where attack windows are the main factor, window-level accuracy may be artificially high and may not translate to reliable real-world detection [28]. Episode-based evaluation provides a more deployment-relevant perspective by measuring detection delay and episode miss rates rather than only window-level accuracy.

In contrast, row-truth evaluation emphasizes the basic difficulty in detecting the attacks at the earliest stage. Row-truth episodes are defined directly from contiguous malicious flows so that they are a stricter and more realistic scenario. Based on this definition, both models only could detect part of the episodes, proving that attack traffic in early stages is often similar to the behavior of benign traffic before the appearance of abnormal intensity or protocol signatures becomes evident. While the coverage of detection was similar in case of both models, Although overall episode detection coverage is identical under row-truth evaluation, CNN–LSTM exhibits slightly lower mean detection delay than CNN-only, suggesting marginally improved stability against late detections and CNN-only model exhibited extreme outliers of delay, leading to heavy tailed delay behavior. Attack type had a strong influence on the dynamics of detection. SYN floods were detectable almost immediately because of the distinctive protocol-flag signatures and UDP floods caused longer delays because early bursts appear to be benign high volume UDP traffic. Near-binary detection behavior was further confirmed by time-budget analysis: there were episodes that were immediately detected and those ones that were never detected despite the long period of observation. Overall, the results reinforce the need for episode-based evaluation to achieve realistic evaluation and that the CNN–LSTM provides improved temporal stability and robustness for real-time DDoS detection.

## *6. Conclusion*

This research studied the effectiveness of deep learning based architectures for the early detection of Distributed Denial-of-Service (DDoS) attacks using flow level traffic data from CIC-DDoS2019 dataset. Unlike traditional research efforts focused mainly on window-level accuracy evaluation, this effort focused more on episode-based evaluation

to evaluate how fast and reliable attacks can be detected after their onset under realistic operational conditions. Two models were considered, CNN-only as a baseline and CNN-LSTM as a hybrid model. Window-level experiments showed that both models have good binary classification performance, especially when testing conditions are balanced. However all these results also proved that high accuracy and AUC scores can be misleading in case of highly imbalanced datasets like is the case in real life DDoS scenarios. As a consequence, in performance assessment of deployment readiness, window-level performance was found to be inadequate. Evaluation based on episodes yielded more information on early detection behavior. Both models exhibited low detection delays and high episode coverage on the definitions of window-truth episode, and this implies that there is good detection reliability once sustained attack behavior has occurred. Under the more stringent row-truth episode definition, which is closer to how attacks appear in the real world, detection was made much more difficult. In this environment, neither of the two models could identify a large portion of the episodes, which underscores the challenge of identifying attacks at the initial stages of their development. Still, the CNN-LSTM model had more stable temporal behaviour and lower extreme detection delays, which is the advantage of including the sequential memory. These findings confirm that while CNN–LSTM improves classification reliability, strict episode-based evaluation reveals that true onset-level early detection remains a challenging open problem.

## *References*

[1]. A. Ahmim, F. Maazouzi, M. Ahmim, S. Namane, and I. B. Dhaou, "Distributed denial of service attack detection for the Internet of Things using hybrid deep learning model," IEEE Access, vol. 11, pp. 119862–119875, 2023.

[2]. M. Ramzan, M. Shoaib, A. Altaf, S. Arshad, F. Iqbal, Á. K. Castilla, and I. Ashraf, "Distributed denial of service attack detection in network traffic using deep learning algorithm," Sensors, vol. 23, no. 20, p. 8642, 2023.

[3]. W. G. Gadallah, H. M. Ibrahim, and N. M. Omar, "A deep learning technique to detect distributed denial of service attacks in software-defined networks," Computers & Security, vol. 137, p. 103588, 2024.

[4]. S. Mohan, S. Nandhini, and K. Gunaseelan, "Detection of denial-of-service attack using a novel hybrid learning technique," Journal of Information Security and Applications, vol. 92, p. 104081, 2025.

[5]. F. M. Aswad, A. M. S. Ahmed, N. A. M. Alhammadi, B. A. Khalaf, and S. A. Mostafa, "Deep learning in distributed denial-of-service attacks detection method for Internet of Things networks," Journal of Intelligent Systems, vol. 32, no. 1, p. 20220155, 2023.

[6]. N. Jayakrishna and N. N. Prasanth, "A hybrid deep learning model for detection and mitigation of DDoS attacks in VANETs," Scientific Reports, vol. 15, no. 1, p. 34170, 2025.

[7]. A. Sharma, S. Rani, S. H. Shah, R. Sharma, F. Yu, and M. M. Hassan, "An efficient hybrid deep learning model for denial of service detection in cyber physical systems," IEEE Transactions on Network Science and Engineering, vol. 10, no. 5, pp. 2419–2428, 2023.

[8]. T. H. Aldhyani and H. Alkahtani, "Cyber security for detecting distributed denial of service attacks in agriculture 4.0: Deep learning model," Mathematics, vol. 11, no. 1, p. 233, 2023.

[9]. E. Deniz and S. Serttaş, "Deep learning-based distributed denial of service detection system in the cloud network," Journal of Scientific Reports-A, no. 055, pp. 16–33, 2023.

[10]. A. Yadav, M. Kaur, C. Sharma, and D. Prashar, "Next-gen distributed denial-of-service detection and mitigation in software-defined networking using hybrid machine learning approach," in Soft Computing in Smart Manufacturing and Materials. Elsevier, 2025, pp. 97–133.

[11]. Y. A. Abid, J. Wu, G. Xu, S. Fu, and M. Waqas, "Multilevel deep neural network approach for enhanced distributed denial-of-service attack detection and classification in software-defined Internet of Things networks," IEEE Internet of Things Journal, vol. 11, no. 14, pp. 24715–24725, 2024.

[12]. N. S. Musa, N. M. Mirza, S. H. Rafique, A. M. Abdallah, and T. Murugan, "Machine learning and deep learning techniques for distributed denial of service anomaly detection in software defined networks—current research solutions," IEEE Access, vol. 12, pp. 17982–18011, 2024.

[13]. S. Abiramasundari and V. Ramaswamy, "Distributed denial-of-service (DDOS) attack detection using supervised machine learning algorithms," Scientific Reports, vol. 15, no. 1, p. 13098, 2025.

[14]. T. Farid and M. Sirat, "Hybrid of supervised learning and optimization algorithm for optimal detection of IoT distributed denial of service attacks," International Journal of Innovative Computing, vol. 13, no. 1, pp. 1–12, 2023.

[15]. S. Berríos, S. Garcia, P. Hermosilla, and H. Allende-Cid, "A machine-learning-based approach for the detection and mitigation of distributed denial-of-service attacks in Internet of Things environments," Applied Sciences, vol. 15, no. 11, p. 6012, 2025.

[16]. S. Venkatraman, S. Kanthimathi, K. S. Jayasankar, T. P. Jiljith, and R. Jashwanth, "A novel self-attention-enabled weighted ensemble-based convolutional neural network framework for distributed denial of service attack classification," IEEE Access, vol. 12, pp. 151515–151531, 2024.

[17]. M. A. O. Rabah, H. Drid, Y. Medjadba, and M. Rahouti, "Detection and mitigation of distributed denial of service attacks using ensemble learning and honeypots in a novel SDN-UAV network architecture," IEEE Access, 2024.

[18]. N. Mahajan, A. Chauhan, H. Kumar, S. Kaushal, and A. K. Sangaiah, "A deep learning approach to detection and mitigation of distributed denial of service attacks in high availability intelligent transport systems," Mobile Networks and Applications, vol. 27, no. 4, pp. 1423–1443, 2022.

[19]. H. Aydın, Z. Orman, and M. A. Aydın, "A long short-term memory (LSTM)-based distributed denial of service (DDoS) detection and defense system design in public cloud network environment," Computers & Security, vol. 118, p. 102725, 2022.

[20]. N. A. Al-Shukaili, M. L. M. Kiah, and I. Ahmedy, "Optimizing feature selection and deep learning techniques for precise detection of low-rate distributed denial of service (LDDoS) attack," Discover Internet of Things, vol. 5, no. 1, p. 80, 2025.

[21]. M. H. Zaib, F. Bashir, K. N. Qureshi, S. Kausar, M. Rizwan, and G. Jeon, "Deep learning based cyber bullying early detection using distributed denial of service flow," Multimedia Systems, vol. 28, no. 6, pp. 1905–1924, 2022.

[22]. A. Fathima, G. S. Devi, and M. Faizaanuddin, "Improving distributed denial of service attack detection using supervised machine learning," Measurement: Sensors, vol. 30, p. 100911, 2023.

[23]. H. Elubeyd and D. Yiltas-Kaplan, "Hybrid deep learning approach for automatic DoS/DDoS attacks detection in software-defined networks," Applied Sciences, vol. 13, no. 6, p. 3828, 2023.

[24]. F. L. Becerra-Suarez, I. Fernández-Roman, and M. G. Forero, "Improvement of distributed denial of service attack detection through machine learning and data processing," Mathematics, vol. 12, no. 9, p. 1294, 2024.

[25]. C. R. Babu, M. Suneetha, M. A. Ahmed, P. R. Babu, M. K. Ishak, H. K. Alkahtani, and S. M. Mostafa, "Hybridization of synergistic swarm and differential evolution with graph convolutional network for distributed denial of service detection and mitigation in IoT environment," Scientific Reports, vol. 14, no. 1, p. 30868, 2024.

[26]. R. Aboalela, K. H. Allehaibi, N. Alsaadi, A. S. Alorfi, L. A. Maghrabi, E. B. Ashary, et al., "Harnessing feature pruning with optimal deep learning-based distributed denial of service cyberattack detection on IoT environment," Alexandria Engineering Journal, vol. 120, pp. 584–597, 2025.

[27]. U. Islam, A. Muhammad, R. Mansoor, M. S. Hossain, I. Ahmad, E. T. Eldin, et al., "Detection of distributed denial of service (DDoS) attacks in IoT based monitoring system of banking sector using machine learning models," Sustainability, vol. 14, no. 14, p. 8374, 2022.

[28]. Y. B. Sanap and P. G. Aher, "Deep learning method for detecting and mitigating distributed denial of service attacks with imbalanced data," in Proceedings of the 2024 International Conference on Integrated Circuits and Communication Systems (ICICACS), Feb. 2024, pp. 1–8.

[29]. N. J. Shohan, G. Tanbhir, F. Elahi, A. Ullah, and M. N. Sakib, "Enhancing network security: A hybrid approach for detection and mitigation of distributed denial-of-service attacks using machine learning," in International Conference on Advanced Network Technologies and Intelligent Computing, Cham, Switzerland: Springer Nature Switzerland, Dec. 2023, pp. 81–95.

[30]. I. Sharafaldin, A. H. Lashkari, S. Hakak, and A. A. Ghorbani, "Developing realistic distributed denial of service (DDoS) attack dataset and taxonomy," in Proceedings of the 2019 International Carnahan Conference on Security Technology (ICCST), Chennai, India, 2019, pp. 1–8, doi: 10.1109/CCST.2019.8888419.