Xi'an Shiyou Daxue Xuebao (Ziran Kexue Ban)/
Journal of Xi'an Shiyou University, Natural Sciences Edition
ISSN: 1673-064X
E-Publication: Online Open Access
Vol: 68 Issue 07 | 2025
DOI: 10.5281/zenodo.15845090

SMART DDoS DEFENSE: PACKET SKEW ANALYSIS FOR HTTP FLOOD DETECTION

KAMAL ALIEYAN
College of Information Technology, Amman Arab University, Amman, Jordan. Email: k.alieyan@aau.ed.jo

MAMOUN ABU HELOU
Faculty of Administrative and Informatics, Al- Istiqlal University, Palestine. Email: mabuhelou@pass.ps

WAHEEB ABU-ULBAH
Faculty of Administrative and Informatics, Al- Istiqlal University, Palestine. Email: w.abuulbeh@pass.ps

AYMAN GHABEN
College of Information Technology, Amman Arab University, Amman, Jordan.
Email: a.ghaben@aau.edu.jo

HANI IWIDAT
Faculty of Administrative and Informatics, Al- Istiqlal University, Palestine. Email: hani.iwidat@pass.ps

YOUSEF A. BAKER EL-EBIARY
Faculty of Informatics and Computing, UniSZA, Malaysia. Email: yousefelebiary@unisza.edu.my

Abstract

One of the most harmful orchestrated cyberattacks against online services or computers on the network is the distributed denial of service (DDoS) attack. Although there are numerous ways to spot DDoS attacks, the issue is still widespread. The primary theories about this gap are discussed in this study utilizing mathematical techniques that may efficiently identify HTTP flooding DDoS attacks. This research suggested an efficient mathematical mechanism based on the tendency measurements (i.e., the skew) of the distribution packets to detect the destructive HTTP flooding DDoS packets in the incoming flows in the traffic before reaching the website. The traffic will be divided into aggregated packets based on a given time, then, each aggregated packet will be broken down into equal smaller time called events, after that those events will be divided into groups according to (equal packet size with the same inter arrival time). Using the skew value for each event, this approach will determine the chance of HTTP flooding DDoS attacks occurring within the group. If the skew value is close to value 1 or -1, it is categorized as an HTTP flooding DDoS attack; otherwise, it is considered normal. The suggested mechanism, which outperforms related literature works, yields excellent accuracy rates of 99.12%, according to experimental findings on the CIC DDoS dataset.

Keywords: DDoS Attacks; HTTP Flooding; Online Services; Quantitative Metrics; Networking Security.

1. INTRODUCTION

In recent years, reliance on the Internet across nearly all aspects of human activity has grown significantly. This expansion is propelled by increasing demand from both the public and private sectors, as well as by the rapid proliferation of emerging technologies such as financial technology, smart mobile devices, and Internet of Things (IoT) applications [1][2]. The significant growth in internet-connected devices and their

Xi'an Shiyou Daxue Xuebao (Ziran Kexue Ban)/
Journal of Xi'an Shiyou University, Natural Sciences Edition
ISSN: 1673-064X
E-Publication: Online Open Access
Vol: 68 Issue 07 | 2025
DOI: 10.5281/zenodo.15845090

applications has introduced new challenges, notably an increased susceptibility to a wide range of cyber threats [3]. The Denial of service (DoS) and the distributed denial of service (DDoS) attacks are the most common cyber threats. These types of attacks, which actively target the availability of network services or resources for legal users, are extremely difficult to detect [3][4]. As a result, many organizations are obliged to expend significant time and resources to secure and safeguard their network services against such attacks. However, recognizing and preventing these attacks is difficult due to the dynamic nature of these sorts of attacks and the closeness of the DDoS attacks traffic pattern to regular network traffic. To handle the threat of DDoS attacks, first understand their nature before planning and implementing an effective reply. DDoS attacks are often regarded as the two most hazardous and destructive threats affecting individuals, businesses, and governments alike [3]. DDoS attacks are a continuing problem on the Internet, as proven by ongoing attacks on commercial servers and ISPs. Because of the disruption in network connectivity, many users were unable to access online services and critical network resources such as cloud services, web servers, e-mail servers, and domain name resolvers [4]. DDoS attacks aimed at denying legitimate users access to internet services or resources are the most harmful [5]. From a historical perspective, the first reported DDoS attack appears to have taken place in August 1999. The Yahoo! Internet portal remained unusable for three hours on February 7, the following year, after being targeted by what was then considered the first large-scale DDoS attack. The following day, Amazon, Buy.com, CNN, and eBay were all targeted by DDoS attacks that rendered their web servers inoperable [6].

The main contribution of this mechanism is the use of a set of statistical concepts (mean, median, and standard deviation) to study the shape of the distribution of equal size packet for each event of the aggregated packets using the skew formula to detect HTTP flooding DDOS attacks [7]. Such mechanism aims at enhancing the previous HTTP flooding DDOS attack methods by utilizing logical, statistical, algebraic functions, thus increasing the DDoS attacks detection accuracy.

The remainder of this paper is structured as follows: Section 2 provides a background of the DDoS attacks and briefly highlights the related works. Section 3. Introduced the proposed detection mechanism. Section 4. reports the experimental settings and results. Section 5 concludes this research and outlines future directions.

2. BACKGROUND AND RELATED WORKS

This section first examines DDoS attacks, HTTP flooding DDoS attacks, and the various DDoS attack defense mechanisms. Then it highlights related literature works.

2.1. Denial of Service/Distributed Denial of Service (Dos/DDoS) Attack

DoS and DDoS attacks continue to be a cause of annoyance for both internet service providers and their customers [5]. By disrupting network connectivity between users and the server, these malicious attacks try to prevent legitimate users from obtaining online

Xi'an Shiyou Daxue Xuebao (Ziran Kexue Ban)/
Journal of Xi'an Shiyou University, Natural Sciences Edition
ISSN: 1673-064X
E-Publication: Online Open Access
Vol: 68 Issue 07 | 2025
DOI: 10.5281/zenodo.15845090

services or resources [8][9]. They are often carried out by flooding the target with traffic or delivering specially engineered packets that cause the system to crash, denying legitimate users of online services or network resources [10] [46].

DoS and DDoS attackers commonly target the web servers of high-profile institutions such as banking, commerce, media, government, and trade organizations. Although DoS attacks seldom result in theft or catastrophic loss of data or assets, they impose significant costs on victims in terms of time, money, reputation, and opportunity [11][28][29]. The difference between DoS and DDoS attacks is the number of attack sources. A DoS attack starts with a single attacker, whereas a DDoS attack is initiated by several attackers and occurred several times causing more losses due to the use of botnets to disseminate attacks [12] [30]. DoS and DDoS attacks seek to degrade the quality of target services or servers, or even to totally shut them down [43][27].

Detecting ongoing DDoS and DoS attacks is difficult for a variety of reasons [12][23][24][44]. The detection procedure takes place online, giving security professionals and system administrators a limited time window to notice and validate the attack, which might lead to misclassification. Also, due to the vast number of attack sources, the attack may be started by a heterogeneous device type. Further, typical network preventative measures, such as packet filtering, software parameter adjusting, and rate limitation, would limit the effectiveness in prevention harm to critical network resources [14]. Moreover, because their network data is so similar, it is impossible to distinguish DDoS attacks from flash crowd occurrences. As a result, a reliable and precise method to detect DDoS attacks on the network is required [15] [41]. DDoS attacks are typically classified into three major groups summarized in Table 1.

Table 1: Commonly categorized threshold of DDoS attacks

Attack Category	Description
Volumetric	The main objective of this attack is to flood the target with traffic to exhaust network or hardware resources. This category includes flooding and amplification/reflection attacks. (e.g., [20]).
Protocol Exploitation	This threat type aims to exploit flaws in network protocols by ingesting connection state tables produced by some network devices. (e.g., [21])
Application Layer	Vulnerabilities in application layer protocols such as HTTP and SSL are taken advantage of. These attacks can also target application code that lacks secure coding techniques. They are stealthy and difficult to identify as they use genuine communications (e.g., [22])

2.3. DDoS HTTP Flooding Attacks

DDoS attacks, particularly HTTP flooding attacks, frequently target the application layer, which handles user requests and transmits data to browsers. HTTP is the most often used protocol on the application layer because it allows communication between browsers and servers. An HTTP flood attack attempts to overload a web server with requests, rendering it unavailable to legitimate users. A single attacker or a group of attackers working together may launch a flood of HTTP requests, typically with the assistance of botnets or compromised devices [46].

Xi'an Shiyou Daxue Xuebao (Ziran Kexue Ban)/
Journal of Xi'an Shiyou University, Natural Sciences Edition
ISSN: 1673-064X
E-Publication: Online Open Access
Vol: 68 Issue 07 | 2025
DOI: 10.5281/zenodo.15845090

The "low and slow" attack is a typical tactic used in HTTP flooding attacks in which compromised requests are used to engage the target server in high-quality computations, causing it to consume many resources while being bombarded with multiple HTTP requests. [17]. These attacks may be difficult to detect because the traffic patterns they generate may appear to be legitimate user activity, making it difficult to distinguish which requests are malicious and which are not [18][47].

HTTP flooding attacks can be difficult to detect because they might be considered as valid protocol connections in network traffic. HTTP flooding attacks may leverage holes in application-layer protocols such as HTTP and SSL, as well as flaws in underlying network protocols [19]. Flooding attacks are widespread in HTTP, the most used protocol at the application layer [16, 42]. Furthermore, these attacks often make use of the POST and discover request methods, which are commonly used to send sensitive data to the Internet.

2.4. Related Works

The purpose of this section is to examine studies, techniques, and mechanisms related to the suggested (skew distribution) mechanism. Table 2 summarizes the associated work techniques and mechanisms ([31],[32],[33],[34],[35],[37],[38],[39], and [40]).

Table 2 examens existing studies on the proposed mechanism. It investigates each study's basic principles, performance, and potential limitations. It realized a gap in these earlier approaches because they were focused on detecting HTTP flooding DDoS attacks in traffic via utilizing subset from tendency measurements (mean, mode, median, standard variation, variance, or skew). To address this issue, the tendency measurements must be used on each group to describe the distribution of packets in each event in each of the arriving aggregated packets. Failure to measure them together may result in regular packets being misclassified as abnormal and vice versa.

Table 2: Related work to the proposed mechanism.

Author	Approach	Performance	limitation
[31]	It proposed a method depending on covariance to distinguish between normal and anomalies SYN packets in the traffic.	accuracy is 100%.	There is no theoretical justification provided for the high detection rate as demonstrated in the experiments.
[32]	It proposed a long-range dependent (LRD) as a traffic series to describe traffic engineering and presented an autocorrelation function that can help as a statistical model of LRD traffic.	It did not compute the accuracy.	This research depended on similarity metric only.
[33]	DDoS attacks that changed across multiple networks domains early detected by developing (DCD) distributed change point detection and (CAT) change aggregation trees. Their system was built over attack transit routers to aggregate the flooding	The accuracy rate is about 98%.	It used false alarm rate (false positive and true negative) and used logical, statistical, and calculus only.

Xi'an Shiyou Daxue Xuebao (Ziran Kexue Ban)/
Journal of Xi'an Shiyou University, Natural Sciences Edition
ISSN: 1673-064X
E-Publication: Online Open Access
Vol: 68 Issue 07 | 2025
DOI: 10.5281/zenodo.15845090

	alerts from the routers and then take the final decision by themselves by using normal distribution of the flooding attack packets between them.		
[34]	It defined a multidimensional access matrix to detect the spatial temporal patterns of a normal flash crowd. A novel anomaly detector based on hidden semi-Markov model is proposed to represent the dynamics of access matrix and to detect the attacks.	The accuracy rate is 90%, and False Positive is 1%.	It focused on entropy functions only.
[35]	IP trace back was considered that there was an independent between packets pollution and attack pattern; by discussing the major two methods in IP tracing, (PPM) probabilistic packet making and (DPM) deterministic packet making. They found that there was high similarity between attack flows towards the normal flows.	An accurate traceback is possible within 20 seconds.	This research depended on time metric only.
[37]	It proposed mechanisms with an architecture that consisted of six machine learning (ML) models (J48, Random Tree, REP Tree, Random Forest, Multi-Layer Perceptron (MLP), and Support Vector Machines (SVM)).	accuracy is about 95%.	It used false alarm rate (false positive and true negative) and used logical, statistical, and calculus only.
[38]	It proposed the semi-supervised weighted k-means mechanism to detect HTTP DDoS attacks by using CIC DDoS dataset.	The accuracy rate is 98.86%	It is built based on an entropy function only without merging them with another mathematical function.
[39]	It proposed a machine learning-based DoS/DDoS detection system that presented inferences based on signatures previously extracted from samples of network traffic.	accuracy about 96%.	It focused on using logical, statistical, and probability functions only.
[40]	It proposed using a multi-modal probability distribution to detect DDoS attacks from the collected statistical information at the flow level.	accuracy rate about 97%.	It depended on correctly detecting normal and misclassification rates and did not use any applied functions.

3. TENDENCY MEASUREMENTS-BASED DETECTION MECHANISM

To meet the research aims, this section provides a skew of distribution packets, a mathematical-based approach for identifying HTTP flooding attacks. The suggested method detects DDoS attacks based on HTTP traffic by watching the characteristics of aggregated packets acquired from network traffic within a given time (t). Figure 1 depicts the four phases of the proposed mechanism: (i) data pre-processing, (ii) packets aggregated attributes, and (iii) anomaly-based detection and (v) Rule based DDoS attack decision.

Xi'an Shiyou Daxue Xuebao (Ziran Kexue Ban)/
Journal of Xi'an Shiyou University, Natural Sciences Edition
ISSN: 1673-064X
E-Publication: Online Open Access
Vol: 68 Issue 07 | 2025
DOI: 10.5281/zenodo.15845090

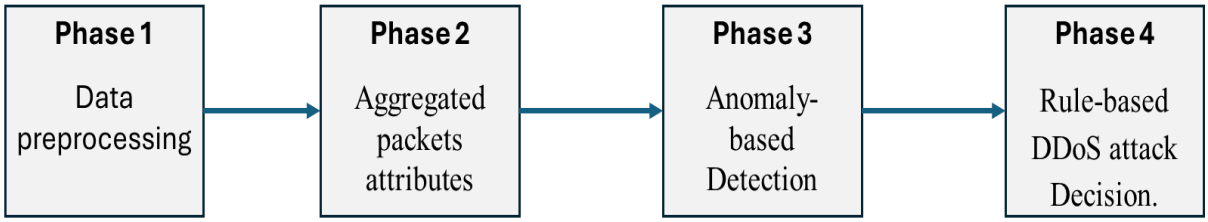

Figure 1: Methodology of the proposed mechanism

3.1 Data pre-processing

This phase receives the collected packets, filters them for HTTP packets, and then cleans the data to remove duplicates. This procedure is divided into two stages: data filtration using Wireshark [52] filtering commands to exclude non-HTTP packets that are not relevant to the research, and data cleansing to remove redundant packets, which are then used as inputs for the next phase [25] [26]. HTTP packets are saved in MySQL database after they are extracted from CSV files (CSV files represent CIC DDoS datasets).

3.1.1 Data Filtration

Not all inbound and outbound network packets are connected and contribute to the detection of HTTP flooding DDoS attacks. As a result, instead of monitoring or observing the complete network traffic, just HTTP activity should be monitored or observed. This decreases the proposed approach's resources overhead. The initial stage is to filter incoming network data to only include HTTP traffic and then extract specific information from the HTTP header. Source IP, destination IP, and packet size are among the extracted features. These traits were chosen based on HTTP traffic experiments and observations, and they are known to aid in the identification of HTTP flooding DDoS attacks. Other scholars, such as [37], [38], and [40], have also employed these qualities in their studies.

3.1.2 Data Cleansing

The data cleansing procedure entails locating and repairing flaws in the data set as well as removing conflicting occurrences. Furthermore, cleaning up the data can increase the accuracy of the findings and reduce the time spent searching for records [48]. Furthermore, the data cleansing procedure restores lost value inside datasets, explains the values of outliers, and corrects any contradictions.

After the data filtering and purification phases are completed, the packets will be used as inputs in the next phase (aggregated packets attributes).

3.2 Aggregated packets attributes

The second phase aggregates the captured packets in each second. The aggregated packets in each $group_{ni}$ will be further split into x events based on time (t). For each $group_{xij}$, the packets will be grouped ($group_{yij}$) based on three attributes: the number of packets, the size of packets, and the regularity of inter-arrival time of packets. As this

Xi'an Shiyou Daxue Xuebao (Ziran Kexue Ban)/
Journal of Xi'an Shiyou University, Natural Sciences Edition
ISSN: 1673-064X
E-Publication: Online Open Access
Vol: 68 Issue 07 | 2025
DOI: 10.5281/zenodo.15845090

mechanism is grounded on events and their values, the purpose for breaking the aggregated packets into events is to prepare them as input of (summation rows-columns) in the next phase. The number of events (x) in each $group_{ni}$ is determined by the experimental and observational results of the HTTP flooding.

3.2.1 Equal packets size

The first attribute seeks to monitor the size of HTTP packets in $event_{xij}$ to assist the suggested approach in detecting HTTP flooding DDoS assaults in each $event_{xij}$ by examining packet sizes. Most HTTP flooding DDoS attacks appear to deliver a slew of identical-sized HTTP packets to the targeted server with the purpose of making it unavailable/unresponsive to genuine users. As a result, the suggested method categorizes incoming HTTP packets in the $event_{xij}$ based on their size. This stage's output is to sort arriving packets into groups based on their size in the (n) group, where n represents the number of unique packet sizes.

3.2.2 Regularity of the packets inter-arrival

The second attribute aims to observe the regularity of the packets' inter-arrival time in each event xij from the previous step through computing the inter-arrival time between each adjacent packet. These adjacent packets must be equal in size.

The inter-arrival time between any two adjacent packets of the same size may be different or equal in the $group_{yij}$ of $event_{xij}$. If inter-arrival time is different, this mechanism will consider this $event_{xij}$ has normal packets; otherwise, $event_{xij}$ has HTTP DDoS attacks, which is the main goal of this research.

The proposed approach relied on the second attribute to detecting the HTTP flooding DDoS attacks in the aggregated packets by computing the inter-arrival time between every equal packet in $group_{yij}$ of $event_{xi}$ (which grouped by the distinct packet size in the previous step).

Users often transmit HTTP packets in standard HTTP requests, i.e., by viewing a certain website, and these requests result in varying packet sizes and inter- arrival times. In contrast to HTTP flooding DDoS assaults, hackers tend to deprive legitimate users of their services by delivering innumerable HTTP packets with equal packet sizes and inter-arrival periods. As a result, in the proposed detection mechanism to detect HTTP DDoS attacks, the quantity of arriving HTTP packets in the $group_{yij}$ is critical for the anomaly-based detection phase.

3.2.3 Number of the packets

The third attribute observes and counts the number of all HTTP packets in each event xij of the aggregated packets groups ($group_{ni}$). The number of the HTTP packets with the same size and the exact interval time in each $group_{yij}$ of $event_{xij}$ is considered the third attribute of the aggregated packets attributes phase.

Xi'an Shiyou Daxue Xuebao (Ziran Kexue Ban)/
Journal of Xi'an Shiyou University, Natural Sciences Edition
ISSN: 1673-064X
E-Publication: Online Open Access
Vol: 68 Issue 07 | 2025
DOI: 10.5281/zenodo.15845090

There is a direct correlation between the number of HTTP packets in $group_{yij}$ of event x_{ij} and the occurrence of HTTP flooding DDoS attacks inside this $event_{xij}$. Therefore, if the $group_{yij}$ has many HTTP packets with the same size packet and interval time, it is used as evidence for HTTP flooding DDoS attacks.

In summary, this phase aggregated packets into n groups within time (t) which are further split into events(x), and each $event_{xij}$ is divided into $group_{yij}$ according to equal packets size. The regularity of the packets inter-arrival time, and the number of packets.

If any $event_{xij}$ exhibits any abnormality, the aggregated packets group n will be considered as HTTP flooding attacks based on the next phase. The three attributes will be passed to the next phase (anomaly-based detection) to detect the presence of HTTP DDoS attacks in the aggregated packets ($group_{yij}$).

3.3 Anomaly-based detection

The third phase uses the proposed indicator (skew of packet distribution) to detect the HTTP DDoS attack within each aggregated packet.

The skew in packet distribution seeks to categorize the (group $_{ni}$) of each aggregated packet event as normal, suspicious, or HTTP flooding DDoS attack by examining distribution shape ($group_{yi}$) and employing tendency measures via the skew value in (Eq.6).

The strength of this indicator (skew of the packets distribution) is its ability to observe the shape of the spread of the HTTP packets of the aggregated packets that captured from the traffic to detect the abnormal behavior of HTPP by dividing the aggregated packets into (event then groups then into intervals) using the statistical measurement of the central tendency (mean, median and standard variation) to compute the skew value for each group by using its intervals, that is, this indicator will work on the event level.

An in-depth examination of the existing systems for detecting DDoS attacks using the Skew of the distribution packets reveals that it uses one or more tendency measurements (mean, mode, median, standard variation, variance, or skew) on all network packets.

However, applying trend measurements to all network packets (regular and abnormal) will result in DDoS attacks being misclassified because all packets in the flow may be of various sizes, implying that they are normal.

To address this issue, this indicator uses tendency measurements on ($group_{yi}$) to find the skew value to reflect the distribution of packets in ($event_i$) reducing the high false-positive of DDoS attacks in these aggregated packets.

The idea of skew of the equal packets size with equal inter-arrival time in the $group_{yij}$ of each $event_{xi}$ is based on the following: mean =median=mode, when $-1 \leq skew \leq 1$ [36], this shape referred to the normal distribution so, the aggregated packets is normal as shown in Figure 2.

Xi'an Shiyou Daxue Xuebao (Ziran Kexue Ban)/
Journal of Xi'an Shiyou University, Natural Sciences Edition
ISSN: 1673-064X
E-Publication: Online Open Access
Vol: 68 Issue 07 | 2025
DOI: 10.5281/zenodo.15845090

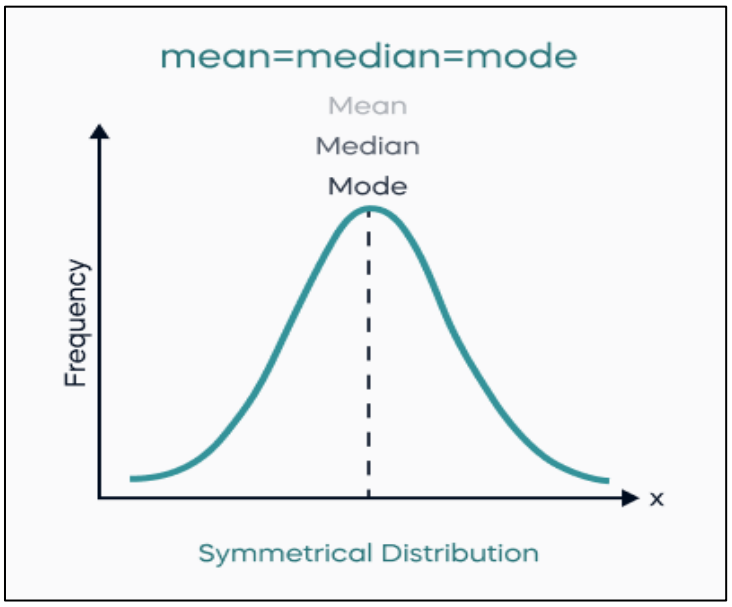

Figure 2: Normal distribution curves [53].

However, if (mean <median<mode), this shape deviated from positive normal distribution (positive skew when *skew* >1, the aggregated packets have HTTP flooding DDoS assault, as shown in Figure 3.

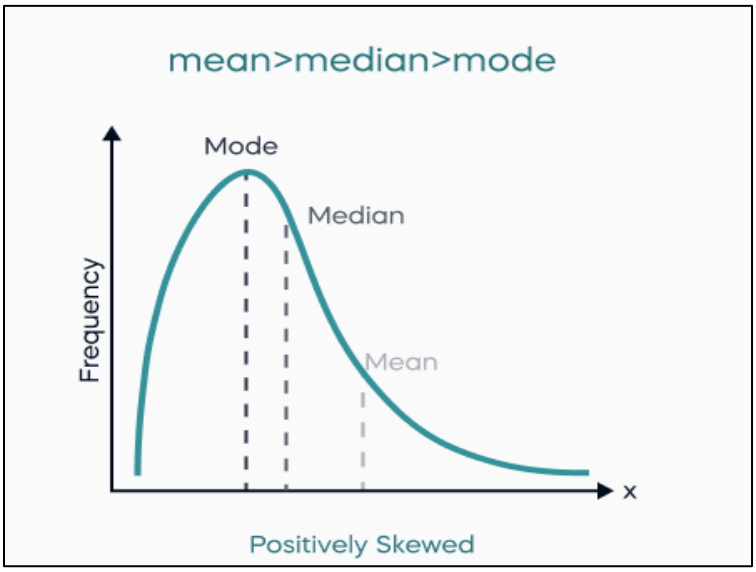

Figure 3: Positive skew curve [53].

And, if (mean >median>mode) this shape diverged from a negative normal distribution (negative skew when *skew* <-1), the aggregated packets were also subjected to an HTTP flooding DDoS attack, as illustrated in Figure 4.

Xi'an Shiyou Daxue Xuebao (Ziran Kexue Ban)/
Journal of Xi'an Shiyou University, Natural Sciences Edition
ISSN: 1673-064X
E-Publication: Online Open Access
Vol: 68 Issue 07 | 2025
DOI: 10.5281/zenodo.15845090

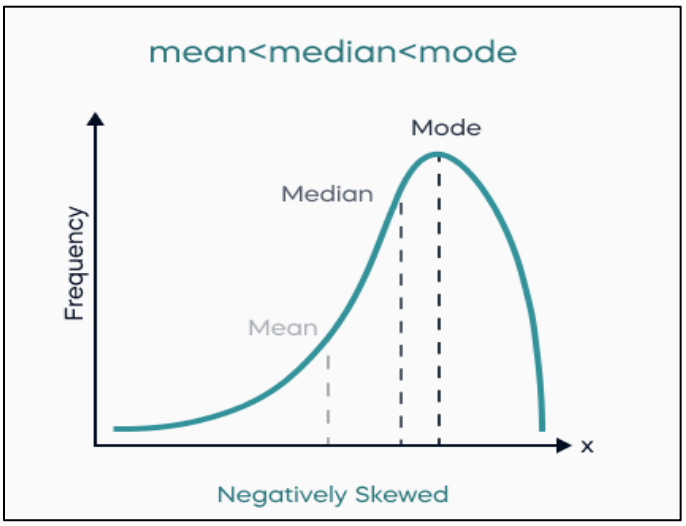

Figure 4: Negative skew curves [53].

The proposed mechanism works according to the following steps:

This indicator divided traffic into aggregated packets each one of them 60 seconds, divided each aggregated packets into events each one of them 5 seconds, divided each event into groups according to the equal packet size and equal inter arrival time then divided each group into intervals each one of them 2.5 seconds to calculate the skew value for each event; because there is several groups in the aggregated packets, the proposed indicator apply the (*OR* operation) on their results to extract the output of the aggregated packet under this indicator.

For each event:

Make a table for each group with its intervals. This indicator computes the mean of the group by building the frequency table of its events through applying the equations:

$$\text{centre of the interval (CoI);}\ \ CoI = \frac{later - begining}{2} \quad (1)$$

$$\bar{X} = \frac{\sum frequency \times CoI}{\sum frequency} \quad (2)$$

It computes the median of the group by building ascending cumulative frequency table of its events by applying the equations:

$$\text{Order of median} = \frac{\sum frequency}{2} \quad (3)$$

$$\text{median} = a + \frac{\text{order of median} - \text{previous cumulative frequency}}{\text{later cumulative frequency} - \text{previous cumulative frequency}} \times l \quad (4)$$

It computes the standard of deviation of the group by using the frequency distribution table and applying the standard variation equation on its events.

Xi'an Shiyou Daxue Xuebao (Ziran Kexue Ban)/
Journal of Xi'an Shiyou University, Natural Sciences Edition
ISSN: 1673-064X
E-Publication: Online Open Access
Vol: 68 Issue 07 | 2025
DOI: 10.5281/zenodo.15845090

$$s = \sqrt{\frac{1}{N}\sum_{i=1}^{N}(x - \bar{x})^2} \quad (5)$$

It computes the skew value of the group through its events by applying the equation:

$$skew = \frac{3(\bar{x} - M)}{s} \quad (6)$$

The skew is used to compare the values of $group_{yij}$ are compared; if (*skew*>1 or *skew*<-1), then ($group_{ni}$) is HTTP DDoS attack; meanwhile, if (-1≤*skew*≤1), then it is normal. It should be noted that, mathematically, if the skew value of the distribution packets (between -1 ≤ *skew* ≤ 1), this distribution is symmetric and it will consider as normal distribution, otherwise, if any lake of symmetry of the normal distribution (when *skew* > 1 or *skew* < -1) this distribution will consider as positive and negative skewness respectively [45]. If the incoming packets in the event of the aggregated packets follow the normal distribution shape, then, this indicator will consider this event as normal, while if the convoy of a massive number of the packets reached in the beginning or ending of the event of the aggregated packet consider as an abnormal distribution as (positive or negative *skew*), this indicator referred to the HTTP DDoS attack.

3.4 Rule based DDoS attack detection.

This phase aims to classify the aggregated packets as either normal, suspicious or HTTP flooding DDoS based on the following rules:

If (*skew*>1 *or skew*<-1) Then:

Output: HTTP flooding DDoS attack

Else (-1≤*skew*≤1) Then:

Output: normal

The decision equation (Eq. 7) collects the group's results then applies an (OR) operation to label the event of the aggregated packets as either DDoS (result = 1), normal (result = 0), or suspicious (result = neglect).

$$Decision\ equation = (result_1\ OR\ result_2\ OR\ \ldots\ OR\ result) \quad (7)$$

If the result of the decision equation is 1, the proposed approach considers the aggregated packets as HTTP flooding attack.

If (Decision = 1) Then:

Output: HTTP flooding DDoS attack

Else if (Decision = 0) Then:

Output: normal

Else:

Output: suspicious

Xi'an Shiyou Daxue Xuebao (Ziran Kexue Ban)/
Journal of Xi'an Shiyou University, Natural Sciences Edition
ISSN: 1673-064X
E-Publication: Online Open Access
Vol: 68 Issue 07 | 2025
DOI: 10.5281/zenodo.15845090

4. EXPERIMENTAL RESULTS

This section introduces the benchmark dataset and the evaluation criteria that will be utilized to apply the proposed technique and subsequently evaluate its accuracy.

4.1 Dataset

This research evaluates the proposed technique using the CIC DDoS dataset (unb.ac/datasets/DDoS-2019.html). The CIC DDoS dataset is a collection of many publicly available non-malicious and malicious datasets from the University of New Brunswick's Canadian Institute for Cyber security (CIC) [50][51]. Table 3 overview the HTTP DDoS traffic in this dataset.

Table 3: Summary of CIC DDoS dataset

Dataset type	Multi-class
Year of formation	2019
Duration of Capture	Ten days
Attack Infrastructure	50 PCs
Victim Infrastructure	420 PCs, 30 servers
Features	80
Number of packets	158,022 packets
Number of normal packets	128,737
Number of malicious packets	29,285 packets

Many machines in the CIC DDoS dataset communicate with the server utilizing DDoS traffic, including HTTP flooding DDoS attacks. The CIC DDoS dataset includes HTTP, HTTPS, FTP, SSH, and email protocol behaviors of 25 individuals [49].

Using aggregated packet properties, the CIC DDoS dataset is labelled to distinguish malicious and non-malicious traffic. Furthermore, as shown in Table 4, all DDoS packet traffic in the CIC DDoS dataset is categorized based on the kind of HTTP GET protocol.

Table 4: List of CIC DDoS Malicious/Non-Malicious and Labelling Machines

IP Address	Traffic Type
192.168.50.8	Malicious / GET HTTP DDoS
192.168.50.5	Malicious / GET HTTP DDoS
192.168.50.6	Malicious / GET HTTP DDoS
192.168.50.7	Malicious / GET HTTP DDoS
192.168.50.9	Non-malicious
192.168.50.6	Non-malicious
192.168.50.7	Non-malicious
192.168.50.8	Non-malicious

4.2 Evaluation metrics

The proposed method employs quantitative criteria to assess the proposed approach's accuracy in identifying HTTP flooding DDoS attacks on web servers. The evaluation metrics (TP, TN, FP, and FN) are adopted. True-positive (TP), which indicates accurately classified harmful traffic. True-negative (TN), which indicates correctly classified normal

Xi'an Shiyou Daxue Xuebao (Ziran Kexue Ban)/
Journal of Xi'an Shiyou University, Natural Sciences Edition
ISSN: 1673-064X
E-Publication: Online Open Access
Vol: 68 Issue 07 | 2025
DOI: 10.5281/zenodo.15845090

traffic, are the quantitative measurements employed. False-positive (FP) traffic is misclassified hostile traffic, and false-negative (FN) traffic is misclassified regular traffic [26][29]. The accuracy of the proposed approach by applying the following equations.

$$Detection\ Accuracy\ (AC) = (TP+TN) / (TP+FP+FN+TN) \times 100 \quad (7)$$

4.3 Experimental environment

Wireshark tool [52] has been used to read the PCAP files of the dataset and filter in the HTTP packets from those aggregated packets and transformed into CSV files, which will be used later as input for the proposed indicator.

Finaly, The HTTP packets are saved in MySQL database. Python is used to implement the proposed approach and process the benchmark datasets as well. Table 5 summarizes the software and hardware specifications used to test the performance of the proposed approach.

Table 5: Experiment environment specification

Hardware	Software
CPU: Intel(R) Core (TM) i5-4670 Memory (RAM): 8.00 GB Hard Drive: 1.0 TB	Operating System: Win7 (64-bit) MySQL server 8.2 Python v 3.9

5. RESULTS AND DISCUSSION

This section tries to assess the suggested mechanism's capacity to identify HTTP flooding DDoS attacks accurately. The assessment is primarily concerned with estimating the detection accuracy.

The threshold (t), which indicates the aggregated packets' time slot, is determined (t) = 60 seconds in this experiment; the choice of (t) is based on earlier research [35][36].

The CIC DDoS dataset, which is separated into 227 aggregated packets, each representing a 60-second time window. As a result, 13,620 (227 x 60) seconds of HTTP traffic are used in this experiment, as shown in Table 6.

Table 6: Aggregated packets of CIC dataset

Number of packets	158,022
Number of the aggregated packets	227
Number of events	2724 (12 x 227)

The quantitative metrics value by applying the proposed mechanism to the 2724 events of the CIC DDoS dataset, namely, the true-positive rate is (99.51%), the false-negative rate is (0.48%), the false-positive rate is (4.76%), and the true-negative rate is (95.23%).

Using Equation 7, the proposed detection accuracy rate is 99.12%. Figure 5 depicts the quantitative metrics analysis (TP, FP, FP, and FN, respectively) on the CIC DDoS dataset.

Xi'an Shiyou Daxue Xuebao (Ziran Kexue Ban)/
Journal of Xi'an Shiyou University, Natural Sciences Edition
ISSN: 1673-064X
E-Publication: Online Open Access
Vol: 68 Issue 07 | 2025
DOI: 10.5281/zenodo.15845090

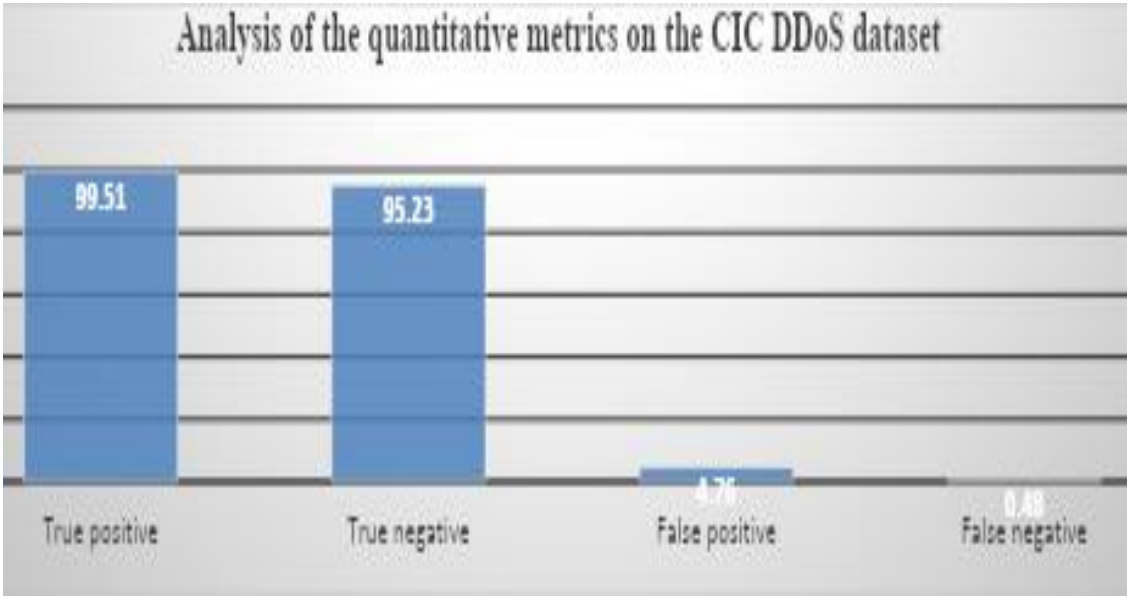

Figure 5: Evaluation metrics of the proposed mechanism using the CIC DDoS dataset

The misclassification occurred because the computed values of (Skew) do not match the predefined thresholds (see, Table 3). However, this mechanism still has strength in detecting the abnormalities in the aggregated packets of this sample due to the small number of misclassification cases. Table 7 reports the comparison between the proposed technique and the existing approaches.

Table 7: Comparison of the accuracy rate on the CIC DDoS dataset

DDoS attack detection approaches	[37]	[38]	The proposed mechanism
Accuracy rate	95%	98.86%	99.12%

Table 7 demonstrations that the detection accuracy rate of the proposed mechanism outperform the comparative approaches ([35] and [36]), indicating that the main hypothesis of this research is correct; that is by using central tendency functions (mean, median, and standard variation) to compute the skew distribution on the captured packets in the aggregated packet from the traffic should improve the detection accuracy.

6. CONCLUSIONS

This research described a mathematical approach for detecting HTTP flooding DDoS attacks. The suggested mechanism computes the skew value for each group of intervals in the aggregated packet from the traffic using statistical measurements of the central tendency (mean, median, and standard variation). The form of packet distribution in aggregated packets in a certain mechanism reflects its efficiency; the more of them used, the better the efficiency, and vice versa. The results demonstrated that the proposed approach is viable and performs better than relevant approaches available in literature.

ISSN: 1673-064X
E-Publication: Online Open Access
Vol: 68 Issue 07 | 2025
DOI: 10.5281/zenodo.15845090

When applied to the CIC DDoS dataset, this work can discriminate between routine, suspicious, and flooding HTTP DDoS attacks in the traffic and reach accuracy rates of 99.12%.

The proposed method is only capable of detecting HTTP flooding DDoS attacks on web servers. Furthermore, the proposed method is based on arriving aggregated network packets rather than the targeted web server's access log file. Several future research directions will focus on application layer protocols (such as MQTT, XMPP, CoAP, and DNS), which are effective fields, especially for security concerns. As a result, there is an urgent need to update security policies and detection techniques in application layer protocols (such as MQTT, XMPP, CoAP, and DNS) before it becomes a severe problem. Further, investigating how combining the proposed mathematical-based method (skewed distribution packets) with network management and security systems might provide value to these applications by improving the accuracy of DDoS attack detection mechanisms.

Author Contributions: Conceptualization, K.A. and A.G; methodology, K.A. and M.A; software, A.G and W.A.; validation, K.A., and M.A.; formal analysis, K.A., and A.G.; investigation, K.A. and M.A; resources, W.A. and H.I.; data curation, W.A and A.G.; writing—original draft preparation, K.A. and A.G.; writing—review and editing, M.A.; visualization, W.A. and H.I.; supervision, K.A.; project administration, K.A.; All authors have read and agreed to the published version of the manuscript.

Funding: Please add: This research received no external funding.

Acknowledgments: The support of the Amman Arab University and Al- Istiqlal University.

Conflicts of Interest: The authors declare no conflicts of interest.

References

1) M. Tehaam, S. Ahmad, H. Shahid, M. S. Saboor, A. Aziz and K. Munir, "A Review of DDoS Attack Detection and Prevention Mechanisms in Clouds," *2022 24th International Multitopic Conference (INMIC)*, Islamabad, Pakistan, 2022, pp. 1-6, doi: 10.1109/INMIC56986.2022.9972962.

2) H. Torres-Carrión, C. Solano-Chamba, C. Narváez-Guillen and M. Cueva-Hurtado, "IoT security issues in the context of Edge Computing: A Systematic Review of Literature," *2022 17th Iberian Conference on Information Systems and Technologies (CISTI)*, Madrid, Spain, 2022, pp. 1-7, doi: 10.23919/CISTI54924.2022.9820159.

3) E. Alomari; S. Manickam; B. B. Gupta; S. Karuppayah; and R. Alfaris. Botnet-based distributed denial of service (DDoS) attacks on web servers: Classification and art. Int. J. Comput Appl. Jul 2012, vol. 49, no. 7, pp. 24_32, doi: 10.5120/7640-0724.

4) K. Park; and H. Lee. On the effectiveness of route-based packet _ltering for distributed DoS attack prevention in power-law internets. ACM SIGCOMM Comput. Commun. Rev 2001, vol. 31, no. 4, pp. 15_26, doi: 10.1145/964723.383061.

5) M. Tayyab; B. Belaton; and M. Anbar. ICMPv6-based DoS and DDoS attacks detection using machine learning techniques, open challenges, and blockchain applicability: A review. IEEE Access 2020. vol. 8, pp. 170529_170547, doi: 10.1109/access.2020.3022963.

6) M. H. Bhuyan; H. J. Kashyap; D. K. Bhattacharyya; and J. K. Kalita. Detecting distributed denial of service attacks: Methods, tools, and future directions. Comput. J.2013, vol. 57, no. 4, pp. 537_556, doi: 10.1093/comjnl/bxt031.

ISSN: 1673-064X
E-Publication: Online Open Access
Vol: 68 Issue 07 | 2025
DOI: 10.5281/zenodo.15845090

7) A. Ghaben, M. Anbar, I. H. Hasbullah and S. Karuppayah, "Mathematical Approach as Qualitative Metrics of Distributed Denial of Service Attack Detection Mechanisms," in *IEEE Access*, vol. 9, pp. 123012-123028, 2021, doi: 10.1109/ACCESS.2021.3110586.

8) Eugenio Borrini, Enrico De Santis, Antonello Rizzi, "A Class Incremental Learning Framework for DDoS Detection", *2025 IEEE Symposium on Computational Intelligence in Security, Defence and Biometrics (CISDB)*, pp.1-9, 2025.

9) A. Bahashwan; M. Anbar; and S. M. Hanshi. Overview of IPv6 Based DDoS and DoS Attacks Detection Mechanisms. Singapore: Springer 2020, vol. 1132.

10) Q.Yan; and F.Yu,. Distributed denial of service attacks in software-defined networking with cloud computing. IEEE Commun. Mag Apr 2015, vol. 53, no. 4, pp. 52_59, doi: 10.1109/MCOM.2015.7081075.

11) M. Darwish; A. Ouda; and L. F. Capretz. Cloud-based DDoS attacks and defenses Marwan. Int. Conf. Inf. Soc. (i-Soc.) Jun. 2013, pp. 67_71.

12) O. E. Elejla; M. Anbar; and B. Belaton. ICMPv6-based DoS and DDoS attacks and defense mechanisms: Review. IETE Tech. Rev Jul. 2017, vol. 34, no. 4, pp. 390_407, doi: 10.1080/02564602.2016.1192964.

13) S. Jin; and D. S. Yeung. A covariance analysis model for DDoS attack detection. IEEE Int. Conf. Commun. Jun. 2004, pp. 1882_1886, doi: 10.1109/icc.2004.1312847.

14) O. E. Elejla; M. Anbar; B. Belaton; and B. O. Alijla. Flow-based IDS for ICMPv6-based DDoS attacks detection. Arabian J. Sci. Eng., Dec 2018, vol. 43, no. 12, pp. 7757_7775, doi: 10.1007/s13369-018-3149-7.

15) O. E. Elejla; B. Belaton; M. Anbar; B. Alabsi; and A. K. Alani. Comparison of classi_cation algorithms on ICMPv6-based DDoS attacks detection. Computational Science and Technology (Lecture Notes in Electrical Engineering), Singapore: Springer Aug. 2018, vol. 481., pp. 347_357, doi: 10.1007/978-981-13-2622-6_34.

16) Karanpreet Singh; Paramvir Singh; and Krishan Kumar. Application layer HTTP-GET flood DDoS attacks: Research landscape and challenges 2017.

17) Karim Afdel; and Mustapha Belouch, Semi-supervised machine learning approach for DDoS detection. Applied Intelligence 2018 – Springer, 2018.

18) Kiwon Hong; Youngjun Kim; Hyungoo Choi; and Jinwoo Park. SDN-Assisted Slow HTTP DDoS Attack Defense Method. Journals & Magazines IEEE Communications Letters 2018, Volume: 22 Issue: 4.

19) Yeonhee Lee; and Youngseok Lee. A Hadoop-Based Packet Trace Processing Tool. J. Domingo-Pascual, Y. Shavitt, and S. Uhlig (Eds.): TMA 2011, LNCS 6613, pp. 51–63. c Springer-Verlag Berlin Heidelberg 2011).

20) Z. Zhang et al., "Revealing Protocol Architecture's Design Patterns in the Volumetric DDoS Defense Design Space," in IEEE Communications Surveys & Tutorials, vol. 27, no. 1, pp. 353-371, Feb. 2025, doi: 10.1109/COMST.2024.3392253.

21) N. K. Singh and S. K. B. J, "Detection and Prevention of UDP Protocol Exploiting and Smurf Attack in WSN Using Sequential Probability Ratio Test Algorithm," 2023 International Conference on Data Science and Network Security (ICDSNS), Tiptur, India, 2023, p. 1-6, doi: 10.1109/ICDSNS58469.2023.10245010.

ISSN: 1673-064X
E-Publication: Online Open Access
Vol: 68 Issue 07 | 2025
DOI: 10.5281/zenodo.15845090

22) Suman, P. S, M. Madiajagan, B. J. J. K. Sagar, S. Selvi and C. Singh, "Detecting Transport and Application Layer DDos Attacks in IoT Devices with Machine and Deep Learning," 2024 International Conference on Communication, Computing and Energy Efficient Technologies (I3CEET), Gautam Buddha Nagar, India, 2024, pp. 1569-1574, doi: 10.1109/I3CEET61722.2024.10993831.

23) G. Zhang; S. Jiang; G. Wei; and Q. Guan. A prediction-based detection algorithm against distributed denial-of-service attacks. J. Univers. Comoput. Sci., Jun 2009, vol. 15, pp. 488_504, doi: 10.1145/1582379.1582403.

24) P. Shamsolmoali; and M. Zareapoor; Statistical based filtering system against DDOS attacks in cloud computing. Int. Conf. Adv. Compute., Commun. Informat. (ICACCI), Sep 2014, pp. 1234_1239, doi: 10.1109/ICACCI.2014.6968282.

25) Y. Purwanto; and B. Rahardjo. Traffic anomaly detection in DDos _cooding attack. 8th Int. Conf. Telecommun. Syst. Services Appl. (TSSA), Oct. 2014, pp. 1_6, doi: 10.1109/TSSA.2014.7065953.

26) R. Jalili; F. Imani-Mehr; M. Amini; and H. R. Shahriari. Detection of distributed denial of service attacks using statistical pre-processor and unsupervised neural networks 1st Int. Conf. Inf. Secur. Pract. Exp. (ISPEC), Apr 2005, vol. 3439, pp. 192_203, doi: 10.1007/978-3-540-31979-5_17.

27) M. Li; and M. Li. A new approach for detecting DDoS attacks based on wavelet analysis. 2nd Int. Congr. Image Signal Process., Oct. 2009, pp. 1_5, doi: 10.1109/CISP.2009.5300903.

28) K. Lee; J. Kim; K. H. Kwon; Y. Han; and S. Kim. DDoS attack detection method using cluster analysis. Expert Syst. Appl., Apr. 2008, vol. 34, no. 3, pp. 1659_1665, doi: 10.1016/j.eswa.2007.01.040.

29) L. Li; and G. Lee. DDoS attack detection and wavelets. Telecommun. Syst., 2005, vol. 28, nos. 3_4, pp. 435_451, doi: 10.1007/s11235-004-5581-0.

30) X. Qin; T. Xu; and C. Wang. DDoS attack detection using _ow entropy and clustering technique. 11th Int. Conf. Comput. Intell. Secur.(CIS), De. 2015, pp. 412_415, doi: 10.1109/CIS.2015.105.

31) Shuyuan Jin; and Daniel S. Yeung, A Covariance Analysis Model for DDoS Attack Detection. IEEE Communications Society, 2004.

32) Ming Li. An approach to reliably identifying signs of DDOS flood Attacks based on LRD traffic pattern recognition. ELSEIER Received 30 January 2004; revised 19 April 2004; accepted 20 April 2004

33) Yu Chen; Kai Hwang; and Wei-Shinn Ku. Collaborative Detection of DDoS Attacks over Multiple Network Domains. Journals & Magazines IEEE Transactions on Parallel 2007, Volume: 18 Issue: 12.

34) Yi Xie; and Shun-Zheng Yu. Monitoring the Application-Layer DDoS Attacks for Popular Websites. IEEE/ACM TRANSACTIONS ON NETWORKING, FEBRUARY 2009, VOL. 17, NO. 1.

35) Shui Yu; Wanlei Zhou; Robin Doss; and Weijia Jia. Traceback of DDoS Attacks using Entropy Variations. Digital Object Indentifier 10.1109/TPDS.2010,.97 1045-9219/10/$26.00 © IEEE, 2011.

36) Jushan BAI; and Serena NG. Tests for Skewness, Kurtosis, and Normality for Time Series Data. © American Statistical Association Journal of Business & Economic Statistics January 2005, Vol. 23, No. 1 DOI 10.1198/073500104000000271, 2005).

37) Perez-Diaz; Jesus Arturo; Ismael Amezcua Valdovinos; Kim Kwang Raymond Choo; and Dakai Zhu. A Flexible SDN-Based Architecture for Identifying and Mitigating Low-Rate DDoS Attacks Using Machine Learning. IEEE Access 2020. 8: 155859–72.

38) Hao Luo; Youzhi Gu; Xingyu Liao; Shenqi Lai; and Wei Jiang. Bag of tricks and a strong baseline for deep person re-identification. Open access, IEEE Explore. 2019.

ISSN: 1673-064X
E-Publication: Online Open Access
Vol: 68 Issue 07 | 2025
DOI: 10.5281/zenodo.15845090

39) Lima Filho; and Francisco Sales De et al. Smart Detection: An Online Approach for DoS/DDoS Attack Detection Using Machine Learning. Security and Communication Networks 2019.

40) Ahmed, Muhammad Ejaz, Saeed Ullah, and Hyoungshick Kim. “Statistical Application Fingerprinting for DDoS Attack Mitigation.” IEEE Transactions on Information Forensics and Security. 2019. 14(6): 1471–84.

41) Malik; and Jahanzaib et al. Hybrid Deep Learning: An Efficient Reconnaissance and Surveillance Detection Mechanism in SDN. IEEE Access 2020, 8: 134695–706.

42) Valdivieso Caraguay; Ángel Leonardo; Alberto Benito Peral; Lorena Isabel; Barona López; and Luis Javier García Villalba. SDN: Evolution and Opportunities in the Development of IoT Applications. Int. Journal of Distributed Sensor Networks 2014.

43) Juan Fernando; Balarezo, Song; Wang Gomez; Chavez Karina; Sithamparanathan Kandeepan; and Akram Al-Hourani. A survey on DoS/DDoS attacks mathematical modelling for traditional SDN and virtual networks. Engineering Science and Technology, an International Journal, July 2022,

44) Adem Karahoca. BotNet Detection: Enhancing Analysis by Using Data Mining Techniques. Advances in Data Mining Knowledge Discovery and Applications 2012.

45) David P. Doane; and Lori E. Seward. Measuring Skewness: A Forgotten Statistic? Journal of Statistics Education 2011. 19:2, DOI: 10.1080/10691898.2011.11889611.

46) Ayman Ghaben; Mohammed Anbar; Iznan Husainy Hasbullah; and Shankar Karuppayah, Mathematical Approach as Qualitative Metrics of Distributed Denial of Service Attack Detection Mechanisms, IEEE Access, September 2021, Digital Object Identifier 10.1109/ACCESS.2021.3110586.

47) Jaafar; Abdullah; & Ismail. Review of Recent Detection Methods for HTTP DDoS Attack. Journal of Computer Networks and Communications 2019, Volume | Article ID 1283472 | https://doi.org/10.1155/2019/1283472.

48) Liu; and Motoda, Data Reduction via Instance Selection. The Springer International Series in Engineering and Computer Science book series (SECS 2001. volume 608).

49) Stefanos Kiourkoulis. DDoS Dataset. Luleå University of Technology Department of Computer Science, Electrical and Space Engineering 2020, 1. https://www.kaggle.com/devendra416/DDoS-datasets/data.

50) Li Junhong. Detection of DDoS Attacks Based on Dense Neural Networks, Autoencoders and Pearson Correlation Coefficient. (April. 2020): 89.

51) Yang, Yanqing et al. Network Intrusion Detection Based on Supervised Adversarial Variational Auto-Encoder with Regularization. IEEE Access 2020. 8: 42169–84.

52) Chappell, Laura. 2012. *Wireshark ®Network Analysis*.

53) 365datascience.com Available online: https://365datascience.com/calculators/skewness-calculator/(accessed on, June 2025).