Mathematical Approach as Qualitative Metrics of Distributed Denial of Service Attack Detection Mechanisms

AYMAN GHABEN, MOHAMMED ANBAR*, (Member, IEEE), IZNAN HUSAINY HASBULLAH*,
AND SHANKAR KARUPPAYAH*
National Advanced IPv6 Centre (NAv6), Universiti Sains Malaysia, Pulau Penang 11800, Malaysia

Corresponding author: Mohammed Anbar (anbar@nav6.usm.my)

This work was supported by the Ministry of Higher Education Malaysia through Fundamental Research Grant Scheme under Project FRGS/1/2019/ICT03/USM/02/3.

ABSTRACT The distributed denial of service (DDoS) attack is one of the most destructive organized cyber-attacks against online services or computers on the network. Despite the existence of many mechanisms to detect DDoS attacks, the problem is still prevalent. This research dissected and analyzed twenty-two existing DDoS attack detection mechanisms, representing all types of DDoS attack defense approaches, to determine the reason for the persistent successful DDoS attacks. This research posits two hypotheses concerning this gap: First, a lack of mathematical function usage by the existing detection mechanisms. The few functions used are limited to logical, statistical, or probability functions, resulting in reduced detection effectiveness. Second, researchers unintentionally or inadvertently miscalculate the mechanisms’ detection accuracy rate by partially using quantitative metrics. This research has three objectives; to propose a set of qualitative metrics based on mathematical functions, to measure the relationship between the quantitative and qualitative metrics in the DDoS attack detection mechanisms, and to prove the relationship between the genuineness of the existing mechanisms’ detection accuracy, and full consideration of quantitative metrics and diversity of qualitative and metrics. The result revealed a correlation rate of 84.22 %, which reflects the correctness of the detection accuracy. Third, identifying the manipulation percentage of reported detection accuracy by employing the correlation rate complement. The result indicated that 15.78 % of the reviewed mechanisms had manipulated or inadvertently miscalculated the accuracy.

INDEX TERMS DDoS attacks, networking security, qualitative metrics, quantitative metrics.

I. INTRODUCTION
The dependency on the Internet for all kinds of human activities has grown exponentially in the last few years. The growth is spurred by demands from all sectors (public and private) and by the vast proliferation of emerging technologies such as smart mobile devices, financial technology (fintech), advanced communication technologies, and the Internet of Things and its applications. Unfortunately, the dramatic increase in Internet-facing devices and applications also brought along many challenges, such as exposure to various cyber threats. The most common cyber threats are denial of service (DoS) and distributed denial of service (DDoS) attacks. These types of attacks deliberately target the availability of network services or resources for legitimate users.

Consequently, many organizations are forced to spend substantial effort and resources to secure and protect their network services from such attacks. However, due to the dynamic nature of these types of attacks and the similarity of the DoS/DDoS attack traffic pattern to regular network traffic, identifying and stopping these attacks are very challenging. Therefore, to address the threat of DoS/DDoS attacks, understanding their nature is a must before designing and engineering an effective counter.

DoS and DDoS attacks are considered the two most dangerous and destructive threats that impact individuals, companies, and governments alike [1]. DoS attack is a persistent Internet problem as evidenced by continuous attacks on commercial servers and ISPs. The disruption of network
connectivity resulted in many users denied access to online services and vital network resources, such as cloud services, web servers, e-mail servers, and domain name resolvers [2]. However, the most damaging attack is DDoS attacks designed to deprive legitimate users of access to online services or resources [3]. The first well-documented DDoS attack appears to have occurred in August 1999. On 7th of February the following year, Yahoo! Internet portal was inaccessible for three hours after being hit by what was then considered the first large-scale DDoS attack. Then, Amazon, Buy.com, CNN, and eBay were all hit by DDoS attacks that incapacitated their web servers the following day [4].

This research has three objectives. First, to propose a set of qualitative metrics that can serve as a guideline for researchers employing a mathematical-based approach to detect DoS/DDoS attacks. Second, to identify the reasons for persistent successful DDoS attacks despite many DoS/DDoS attack detection mechanisms with high accuracy rates existed. The second objective is achieved by performing mathematical analysis using the Spearman rank coefficient. Third, reveal the miscalculation of the reported detection accuracy by employing the complement of the correlation rate.

There are three main contributions of this work. First, a set of qualitative metrics based on the usage of logical operations, mathematical functions, probability functions, algebraic functions, calculus functions, or applied mathematical formula by analyzing the existing mathematical-based DDoS attack detection mechanisms. Second, quantifying the correlation between the existing quantitative metrics and the proposed qualitative metrics using the Spearman rank coefficient. Third, a method to calculate actual percentage of the mechanisms’ detection accuracy using Spearman rank coefficient’s complement percentage.

The remainder of this paper is structured as follows: Section 2 provides the background of the research with subsections on the types of DDoS attacks and the methods of DDoS attack defense mechanisms. Section 3 evaluates the existing related work. Section 4 describes and discusses the evaluation metrics used in this research, including the mathematical approach (the qualitative metrics), quantitative metrics, and the correlation between the quantitative and qualitative metrics. Section 5 describes the research flow, and finally, Section 5 summarizes and concludes this paper. Figure 1 illustrates the organization of this paper.

II. BACKGROUND
This section discusses DoS/DDoS attacks and the various methods employed by DoS/DDoS attack defense mechanisms.

A. DENIAL OF SERVICE/DISTRIBUTED DENIAL OF SERVICE ATTACK
DoS/DDoS attacks continue to cause problems for the internet service providers as well as Internet users. Researchers have been trying to unravel the inner working of DoS/DDoS attacks since its inception [3].

DoS/DDoS attack is a malicious attempt to prevent legitimate users from accessing online services or resources by incapacitating the server that provides the service or bringing down the network connectivity between users and the server [5]. DoS/DDoS attacks accomplish this by flooding the target with traffic or sending specifically crafted packets that trigger a crash. In both instances, the DoS/DDoS attacks deprive legitimate users (i.e., employees, subscribers, or account holders) of the online services or network resources [6].

DoS/DDoS attackers often target web servers of high-profile organizations such as banking, commerce, media companies, or government and trade organizations. Though DoS attacks do not typically result in the theft or significant loss of information or other assets, they can cost the victim a great deal of time and money to handle, its reputation, and lost opportunities [7].

The difference between DoS and DDoS attacks is in the number of attack sources involved. A single attacker triggers a DoS attack. In contrast, multiple attackers trigger a DDoS attack; and by taking advantage of distributed attacks via botnets, a DDoS attack is several times more destructive than DoS [8].

Detecting an ongoing DDoS attack is challenging for several reasons [9]. First, the detection process occurred online, which provides a limited time window for security experts and system administrators to detect and confirm the ongoing
A. Ghaben et al. Mathematical Approach as Qualitative Metrics of DDoS Attack Detection Mechanisms

TABLE 1. Categorization of DDoS attack defense mechanisms based on activity level.

| DDoS defense by activity level | Preventive Attack Prevention | • System security: allow victims to survive attack attempts without refusing services to legitimate users.  
| | | • Protocol Security: tackle bad protocol design problem.  
| | DDoS Prevention | • Resource accounting: services police each user’s access to resources based on the user’s rights and actions.  
| | | • Resource multiplication: offer many tools to combat DDoS attack threats.  
| | Reactive by detection strategy | • Signature-based IDS: deploy pattern detection to store recognized attack signatures in a database.  
| | | • Third-party: implementations do not manage the detection process itself.  
| | | • Anomaly-based IDS: attacks detected based on abnormal traffic behavior vs. attack signature.  
| | | • Hybrid: combine pattern-based detection with anomaly-based detection.  
| | Reactive by response strategy | • Agent identification: provide the identity of the attackers’ machines to the victims.  
| | | • Rate-limiting: impose a limit on traffic rate once detected as malicious.  
| | | • Filtering: makes use of characterization generated by a detection mechanism to filter out the attack stream fully.  
| | Reactive by cooperation degree | • Autonomous: the mechanism conducts independent defense at the point where they are deployed.  
| | | • Cooperative: the mechanism is capable of autonomous detection and response but can achieve significantly better performance through cooperation with other entities.  
| | | • Interdependent: the mechanism relies on other entities for attack prevention or attack detection because it cannot operate independently.

DEFANT attack, which leads to misclassification of the attack. Second, the massive number of attack sources that trigger the attack could comprise a heterogeneous device type. Third, the limited capability of typical network preventive measures (e.g., packet filtering, software parameters tweak, rate-limiting, etc.) despite their usefulness in preventing damages to vital network resources [10]. Finally, it is challenging to distinguish DDoS attacks from flash crowd events due to their network traffic similarity. Therefore, there is a need for an effective and accurate mechanism to detect DDoS attacks in the network [11].

B. METHODS OF DDoS ATTACK DEFENSE MECHANISMS

This section discusses the methods of DDoS attack defense mechanisms, categorized into two groups based on their activity level or location [12].

1) DDoS ATTACK DEFENSE MECHANISMS BASED ON ACTIVITY LEVEL

This section provides the categorization of activity level-based DDoS attack defense mechanisms, as shown in Table 1.

The activity level-based DDoS attack defense mechanisms have two different sub-categories: preventive and reactive. The preventive category has two groups: attack prevention and DDoS prevention, and the reactive category has three groups: detection strategy, response strategy, and cooperation degree [13], [14].

2) DDoS ATTACK DEFENSE MECHANISMS BASED ON LOCATION

The second category of DoS/DDoS attack defense mechanisms is based on the mechanism’s location in the network.

The two sub-categories for location-based DDoS attack defense mechanisms are victim network and intermediate network. The victim network category is for mechanisms that run on the victim network, whereas the second sub-category is for mechanisms deployed in the intermediate network [12], [15].

III. RELATED WORKS

There are many mechanisms have been proposed to detect DDoS attacks, such as machine learning and the mathematical based mechanisms. The difference between mathematical-based DDoS detection mechanism and machine learning-based DDoS detection mechanism is that machine learning-based mechanism aims to predict future events or classify an existing material based on training data, i.e., to classify the network traffic as normal traffic or DDoS attacks. On the other hand, mathematical-based DDoS detection mechanism aims to find the relationship between the data points, i.e., find the relationship between two or more features that represent the network traffic.

Gogoi et al. categorized DDoS attack defense mechanisms into four categories: statistical technique, soft computational...
technique, knowledge-based methods, and clustering [16], as shown in Figure 3.

A. STATISTICAL TECHNIQUES
The first category comprises DDoS attack defense mechanisms utilizing statistical-based techniques that generate a statistical model based on a given data [17]. The resulting model is used as the prediction model to classify new incoming data. The unknown instances are detected based on a statistical inference test to decide if it belongs to that model. Table 2 summarizes the existing DDoS attack detection mechanisms employing statistical-based techniques.

B. SOFT COMPUTING TECHNIQUES
The second category comprises DDoS attack defense mechanisms based on soft computing techniques. Soft computing technique applies problem-solving techniques, such as fuzzy logic, probabilistic reasoning, neural networks, and genetic algorithms (Ibrahim Goni & Ahmed Lawal, 2015). Table 3 summarizes the existing DDoS attack detection mechanisms employing soft computing-based techniques.

C. KNOWLEDGE-BASED METHODS
The third category comprises DDoS attack mechanisms utilizing knowledge-based techniques. Knowledge-based techniques attempt to match the traffic or flow patterns against a set of predefined rules. The traffic or flow is flagged as an attack if it fits the rules. Otherwise, the pattern is considered normal. Table 4 summarizes the existing DDoS attack detection mechanisms employing knowledge-based techniques [4].

D. CLUSTERING TECHNIQUES DDoS ATTACK MECHANISMS
The fourth category of DDoS attack mechanisms is clustering-based techniques, a data mining technique known as unsupervised classification. It does not need training with a training dataset, and the strength of clustering is within the algorithm itself. Table 5 summarizes the existing DDoS attack mechanisms employing clustering-based techniques.

After researching the nature of DDoS attacks, DDoS attack detection mechanisms, and comparisons, the paper classified the weaknesses of existing DDoS attack mechanisms based on the taxonomy of [16]. The classified mathematical-based approach is the feeder or input for the next stage.

IV. PROPOSED EVALUATION METRICS
In this paper, both qualitative and quantitative metrics are used to evaluate the existing DDoS attack detection mechanisms in terms of mathematical functions’ level of use and accuracy calculation correctness. The details of each metric are in the following subsections.

A. QUALITATIVE METRICS
This section discusses the proposed qualitative metrics based on the study of existing DDoS attack detection mechanisms listed in Section 3. The existing mathematical-based DDoS attack detection mechanisms use various mathematical functions, formulas, and logical operations. The study revealed that the existing DDoS attack detection mechanisms could be classified based on five primary mathematical categories: logical operations, statistical functions, probability functions, algebraic functions, and calculus functions.

1) CATEGORY 1 (LOGICAL OPERATIONS) indicates the degree of logical operation usage in DDoS attack mechanisms. Logical operations are simple arithmetic operations, such as addition, subtraction, multiplication, division, and comparison operations, such as similar, the biggest, the least, max, min, and counts. Mathematical operation on port number, protocol number, number of packets, number of flows, threshold comparison, packet size, data size, etc., typically uses logical operations.

2) CATEGORY 2 (STATISTICAL FUNCTIONS) indicates the degree of statistical function usage in DDoS attack mechanisms. Statistical functions include the average, mean, median, mode, variance, standard deviation, percentage, hypothesis, etc. Some examples of statistical function usage are for calculating the average entropy, normalization, and Euclidian distance.

3) CATEGORY 3 (PROBABILITY FUNCTIONS) indicates the degree of probability function usage in DDoS attack mechanisms. Probability functions include the probability of events, conditional probability, the theory of entropy naïve Bayes, normal distribution, distribution of poisons, distribution of Chi, and expected function. Probability functions usually are used to calculate the entropy, probability density function, etc.
### Table 2: Existing DDoS attack mechanisms employing statistical-based techniques.

| Author | Year of the proposed mechanism | Main Idea | Mathematical Functions Used | Experimental Results | Drawbacks |
|--------|-------------------------------|-----------|-----------------------------|---------------------|-----------|
| [18]   | 2017                          | The DDoS attacks in the traffic were presented mathematically through equal inter-arrival time between two adjacent packets using resources’ total probability depletion function at the victim’s end. | $p^0 = \left( \frac{a_i^A}{a_i} + a_i^N \right) \frac{a_i^N}{a_i}$  
$p^m = \frac{\mu^M_{\text{total}}}{\mu^M_{\text{total}}} \sum p_i^m$  
$a = (\beta_\alpha + \beta_\lambda) / \mu^M_{\text{total}}$  
$Y = \mu_A + \mu_N = \frac{\delta_{MA}}{t_{MA}} + \frac{\delta_{MN}}{t_{MN}}$ | It does not compute detection accuracy. | Describe DDoS attack as equal packet size with equal inter-arrival time without considering packet content. |
| [19]   | 2015                          | It evaluated several information metrics, Hartley entropy, Shannon entropy, Renyi entropy, generalized entropy, Kullback-Leibler divergence, and generalized knowledge distance measures to detect low-rate and high-rate DDoS attacks. | $H_1(x) = -\sum_{i=1}^{n} p_i \log_2 p_i$  
$D_k(p \mid q) = \frac{1}{2\pi} \log_2 \left( \sum_{i=1}^{n} p_i q_i^{1-k} \right)$  
$D_0(p \mid q) = -\log_2 \left( \sum_{i=1}^{n} q_i \right)$ | It does not compute detection accuracy. | It focuses only on the entropy equation and does not compute the detection accuracy. |
| [20]   | 2014                          | It presented a statistical technique to detect and filter DDOS attacks to mitigate most TCP attacks. | $D_t = \sum p_i \times \log \frac{p_i}{q_i}$  
$m = \frac{1}{2} - (p + q)$ | It neglects true-negative in detection accuracy calculation. | This mechanism only measures false-positive. |
| [21]   | 2009                          | It proposed a prediction method for the protected server’s available service rate by applying the Auto-Regressive Integrated Moving Average (ARIMA) model. | $\hat{p}_k = \frac{a_k}{a^{\text{new}}}$  
$r_k = \frac{a_k}{a_{k-1}} \frac{a_{k-1}}{a_{k-2}} \frac{a_{k-2}}{a_{k-3}} \cdots \frac{a_2}{a_1}$  
$\text{var}[a_k] = \sigma^2$  
$\hat{p}_k(1) = \left( 1 + \theta \right) p_k - \theta \hat{p}_{k-1}$  
$\sigma^2 = \frac{a_k}{a^{\text{new}}}$  
$\theta = \frac{a_k}{a_{k-1}} \frac{a_{k-1}}{a_{k-2}} \frac{a_{k-2}}{a_{k-3}} \cdots \frac{a_2}{a_1}$  
$\theta = \frac{c_0}{d_0}$  
$(p_{1+k} - \hat{p}_k)$, $k=0,1,2$  
$\sigma^2 = \frac{c_0}{d_0}$  
$\theta = -\frac{c_0}{d_0}$ | The results show that for most predictions, the relative errors are about 1. | This research relied only on precision as efficiency/efficiency metrics. It did not measure false-positive and false-negative and only used rational, statistical, and probability functions. |
| [22]   | 2009                          | It is based on the difference between normal SYN arrival rate (SAR) and SAR attack. The proposed approach used standard SAR statistics, and it confirms the normal distribution flow. | $X = \frac{\sum_{i=1}^{N} x_i}{N}$  
$S^2 = \frac{\sum_{i=1}^{N} (x_i - \bar{x})^2}{N-1}$  
$S = \sqrt{S^2}$ | It indicates that false-positive and false-negative possibilities are very slight, SAR FNR and RA = 99.99%. | This research relied on two efficacy/efficiency measures. It did not measure detection accuracy and only used logical and statistical functions. |
| [23]   | 2007                          | It built a distributed change-point detection (DCD) architecture using change aggregation trees (CAT) to detect abrupt traffic changes through multiple network domains at the earliest time. | $\hat{\chi}(m_t, l) = \left( 1 - \alpha \right) \hat{\chi}(m_{t-1}, l) + \alpha \cdot x(t_m, l)$  
$S_{l_{\text{in}}} = \max \left\{ 0, S_{l_{\text{in}}}(m_{t-1}, l) + \chi(t_m, l) \right\}$  
$DFA_{l_{\text{in}}}(m_t, l) = S_{l_{\text{in}}}(m_t, l) / \hat{\chi}(m_t, l)$ | It shows that four network domains are adequate with just 1 percent false-positive alarms to yield 98% detection accuracy. | It did not calculate false-negative and used only logical and statistical functions. |
4) CATEGORY 4 (ALGEBRAIC FUNCTIONS) indicates the degree of algebraic function usage in DDoS attack mechanisms related to matrices, vectors, determinants, etc. Some examples of algebraic function usage include the calculation of discrete Fourier transform (DFT), discrete wavelet transforms (DWT), list, DFT matrix, DWT matrix, norms, etc.

5) CATEGORY 5 (CALCULUS FUNCTIONS) indicates the degree of the use of calculus functions in DDoS attack mechanisms, which includes sequences, series, limits, derivatives, integrals, etc., and used for integrals in DFT, DWT, summation, product, HaarR, Laplace transform, differential equations, etc.

Other than the five categories listed above, the applied mathematical formula is a mathematical category used in different fields and shows impressive results but not yet widely used or adopted for detecting DDoS attack, as shown in the reported analysis in Table 5 to Table 9. Therefore, we propose adding mathematical formulas as a new qualitative metric under Category 6.

6) CATEGORY 6 (APPLIED MATHEMATICAL FORMULA) indicates the degree of applied mathematical formula usage in DDoS attack mechanisms. These formulas are widely used in other research fields to calculate Reynold’s number in fluid mechanics, Ohm’s law, and Bernoulli’s principle and showed impressive results.

The proposed quantitative metrics evaluate the mechanisms discussed in Section 3 by enumerating mathematical functions (the qualitative matrices) used by each mechanism. The results of the evaluation of existing DDoS attack detection mechanisms employing statistical-based techniques, soft-computing, knowledge-based methods, and clustering are shown in Table 6, 7, 8, and 9, respectively. All the numbers tabulated in the tables represent the number of mathematical functions used by each mechanism.

Table 6 shows that the algebraic function is the most used mathematical function by mechanisms based on statistical...
### TABLE 4. Existing DDoS attack mechanisms employing the knowledge-based technique.

| Author | Year of the proposed mechanism | Main Idea | Mathematical functions used | Experimental results | Drawbacks |
|--------|-------------------------------|-----------|----------------------------|----------------------|-----------|
| [28]   | 2013                          | Build computational algorithms to harmonize emerging battery-driven ECG patterns and evaluate long-term signals in a time-efficient manner. | $y[n] = (x[n])^2$ $MA_{\text{alert}}[n] = \frac{1}{w_2} (y\left[ n - \frac{(w_2-1)}{2} \right] + \cdots + y[n] + \frac{(w_2-1)}{2})$ | The detector’s speed in over 130-minute recordings is approximately 2.2 seconds. | It neglected true-negative in accuracy calculation and depended on the detector’s speed to measure the accuracy. |
| [29]   | 2013                          | combine existing concepts with new IDS techniques by merging entropy. | $p(x) = \frac{\text{number of flows with flow size}}{\text{total number of packets}}$ $H(x) = \frac{1}{n} H(x_1, x_2, \ldots, x_n)$ | A detection accuracy rate was not provided. | No evidence on computation efficiency provided. |
| [30]   | 2007                          | Leverage DDoS attacks’ spatial and temporal similarity. | $P(F, x) = \prod_{i} P(f_1 \backslash x_i) P(x_i)$ | It could detect DDoS attacks with a 97% detection accuracy. | It did not quantify false-negative and accuracy and used only the logical and mathematical functions and probability functions. |
| [31]   | 2004                          | Examine TCP/IP packet header against well-defined rules and conditions and distinguishes normal and abnormal traffic. | $\text{Ratio} = \frac{\text{Total number of incoming packets}}{\text{Total number of outgoing packets}}$ | No detection accuracy rates were provided. | The finding of this mechanism was not reported, and it only used logical and mathematical functions. |
| [32]   | 2003                          | Propose a revolutionary set of technologies to allow organizations to defend against DDoS attacks that can meet high bandwidth, scalability, and performance needs. | Legitimacy-weight = f (assurance, reliability, strength) | Detection accuracy rates not provided. | False-positive and false-negative rates not provided. |

Table 7 shows that the probability function is the most used mathematical function in soft computing-based detection techniques with seven occurrences, while logical operations are the least used with 0%. Only one mechanism in the category uses the applied mathematical formula. In terms of diversity, the mechanism by [21] utilized the most diverse mathematical functions in this category with three different types of mathematical functions and operations, and [20] used the least.

Table 7 shows that the probability function is the most used mathematical function in soft computing-based detection techniques with seven occurrences, while logical operations are the least used. The mechanism by [24] uses the most diverse mathematical functions in the soft computing-based category with four different mathematical functions and operations, while the mechanism by [37] and [38] used only one type of them.

Table 8 shows that the probability function is the most used mathematical function in the knowledge-based technique category with six calls. No mechanism in this category uses the calculus function and applied mathematical function. The mechanisms by [28] and [32] use two different mathematical functions, while the others only used one.

Table 9 shows that the calculus function is the most used mathematical function in the mechanisms based on clustering techniques with eight calls. However, none uses the logical operation or applied mathematical formula in this category. Two mechanisms by [34] and [35] used three different mathematical functions, while [36] and [33] only use one.

### B. THE QUANTITATIVE METRICS

The quantitative metrics used are false-positive (FP), false-negative (FN), true-positive (TP), and true-negative (TN). These four metrics quantify any detection mechanism’s accuracy.

Detection accuracy evaluates the DDoS attack detection mechanism’s accuracy in triggering the alert in the presence of a DDoS attack in the network traffic. Equation (1) is the formula to calculate the accuracy of the DDoS attack.
TABLE 5. Existing DDoS attack mechanisms employing clustering-based techniques.

| Author        | Year of the proposed mechanism | Main Idea                                                                 |
|---------------|---------------------------------|---------------------------------------------------------------------------|
| [33]          | 2015                            | Construct entropy vectors of various traffic flow features, using a clustering analysis algorithm to model normal patterns and then creating models by detecting deviations. |
| [6]           | 2015                            | It considers users ask for frequency series as a sparse matrix, then applying sparse vector decomposition and matching rhythm (SVD-RM), based on sparse vector decomposition and corresponding rhythm proposed as an embedded classifier in SVD-RM, before making the simulation. |
| [34]          | 2009                            | Use discrete wavelet transformation (DWT), continuous wavelet transformation (CWT), and discrete wavelet transformation (DWT). The difference is that the former calculates the correspondence for each lag at every possible scale. |
| [35]          | 2008                            | Detect each step of the DDoS attack separately. The DDoS attack features collect traffic variables that provide information on each phase of the DDoS attack frequency. |
| [36]          | 2005                            | Use wavelet-based energy distribution to detect DDoS.                      |

Mathematical Functions Used

\( H(x) = - \sum_{i=1}^{n} \left( \frac{\hat{\theta}_i}{\theta} \right) \log\left( \frac{\hat{\theta}_i}{\theta} \right) \)

\( \text{Rate} = \frac{\text{the detection rate}}{\text{the false positive rate}} \)

\( \text{Detection Accuracy} = \frac{TP + TN}{TP + FP + FN + TN} \times 100 \)  

\( \text{Total accuracy rate: } 92.4\% \text{ (Type 2) and } 89.21\% \text{ (Type 3) and detection rate: } 91.3\% \text{ (Type 2) and } 88.67\% \text{ (Type 3).} \)

Drawbacks

- It depends only on the false-positive rate in detection accuracy calculation but neglects true-positive. It only depends on the entropy equation.
- It relies on false-positive detection accuracy rate only and ignores true-negative.
- The finding of this mechanism was not reported.
- It does not rely on any efficacy/efficiency metrics, has not measured false negatives, and uses logical and statistical functions and probability functions only.
- It did not measure false negatives, false positives and use only the features of logical and mathematical features, algebraic functions, and calculus analysis.

Unfortunately, mechanisms’ detection accuracy is wrongly calculated by ignoring some of the quantitative metrics in the calculation instead of considering all quantitative metrics. Only the calculations that employ all quantitative metrics will achieve a genuine detection accuracy measure. Therefore, detection accuracy’s genuineness is proposed as a new quantitative metric to validate the claimed detection accuracy.

Equation (2) is the formula to calculate the genuineness of detection accuracy.

\[ \text{Genuineness of detection accuracy} = \frac{\text{number of metrics used in the mechanism}}{\text{Total number of metrics}} \]  

The genuineness of the detection accuracy formula above validates the mathematical-based DDoS attack detection mechanisms listed in Section 3.
C. CORRELATION BETWEEN THE QUALITATIVE AND QUANTITATIVE METRICS

This research follows three steps to prove the relationship between the proposed qualitative metrics and the existing quantitative metrics. First, analyzing twenty-two existing DDoS attack detection mechanisms using qualitative metrics. Second, using the quantitative metrics to analyze the twenty-two existing DDoS attack detection mechanisms. Third, measuring the correlation between the qualitative and quantitative metrics by employing the Spearman rank correlation to determine the relationship strength. The details of the three steps are in the following subsections.

1) QUALITATIVE ANALYSIS OF DDoS ATTACK DETECTION MECHANISMS

In this section, the proposed qualitative metrics (logical operations, statistical functions, probability functions, algebraic functions, and calculus functions) are applied to the existing DDoS attack detection mechanisms. The following tables provide a quantitative evaluation of the mechanisms using the proposed metrics.

TABLE 7. Evaluation of existing DDoS attack detection mechanisms employing soft computing-based techniques using proposed quantitative metrics.

| Qualitative Metrics | Logical operation | Statistical function | Probability function | Algebraic function | Calculus function | Number of operations/functions used |
|---------------------|-------------------|----------------------|----------------------|-------------------|------------------|-------------------------------------|
| [24]                | 1                 | 0                    | 2                    | 4                 | 3                | 0                                  |
| [37]                | 0                 | 0                    | 0                    | 1                 | 0                | 0                                  |
| [25]                | 0                 | 0                    | 4                    | 0                 | 0                | 0                                  |
| [26]                | 1                 | 1                    | 1                    | 0                 | 1                | 0                                  |
| [38]                | 0                 | 1                    | 0                    | 0                 | 0                | 0                                  |
| [27]                | 1                 | 1                    | 0                    | 0                 | 0                | 2                                  |
| Number of times used| 3                 | 2                    | 7                    | 5                 | 4                | 0                                  |

TABLE 8. Evaluation of existing DDoS attack detection mechanisms employing knowledge-based techniques using proposed quantitative metrics.

| Qualitative Metrics | Logical operation | Statistical function | Probability function | Algebraic function | Calculus function | Number of operations/functions used |
|---------------------|-------------------|----------------------|----------------------|-------------------|------------------|-------------------------------------|
| [28]                | 0                 | 1                    | 0                    | 5                 | 0                | 0                                  |
| [29]                | 0                 | 0                    | 4                    | 0                 | 0                | 0                                  |
| [30]                | 0                 | 0                    | 2                    | 0                 | 0                | 0                                  |
| [31]                | 0                 | 3                    | 0                    | 0                 | 0                | 1                                  |
| [32]                | 1                 | 1                    | 0                    | 0                 | 0                | 0                                  |
| Number of times used| 1                 | 5                    | 6                    | 5                 | 0                | 0                                  |
functions, and calculus analysis) measure the degree of mathematical operation and functions used by twenty-two existing DDoS detection mechanisms. Table 11 to Table 14 show the analysis of existing DDoS detection mechanisms using the proposed qualitative metrics.

This research reviewed the DDoS attack mechanisms tabulated in Table 6 through Table 9 to create descriptive data using true (T) or false (F) labels. A T label is assigned if the particular mechanism uses a particular qualitative metric; otherwise, it is assigned an F label. Then, the descriptive data is converted into its equivalent numerical value (0 or 1). A value of 1 is assigned to a mechanism if it uses any mathematical operations, function, or formulas, and 0 otherwise.

So, the values are added together to obtain the total, which will be the input for the Spearman coefficient calculation.

The research computed the percentage of qualitative metrics used in each DDoS attack mechanism by using Equation (3).

Percentage of qualitative metrics used

\[
\text{Percentage of qualitative metrics used} = \frac{\text{number of metrics used}}{\text{Total number of the metrics}}
\]  

(3)

The research also computed the percentage of the mechanisms using the qualitative metrics by using Equation (4).

\[
\text{Percentage of mechanisms using qualitative metrics} = \frac{\text{number of mechanisms using qualitative metrics}}{\text{Total number of mechanisms}}
\]  

(4)

Table 11 shows that the probability function is the most frequently used mathematical operation by mechanisms employing statistical-based detection techniques with four occurrences, or equivalent to 66.6 % of the mechanisms. Meanwhile, no mechanism in this category uses logical operation, and only [23] uses the applied mathematical formula. The mechanism by [18] and [21] are the two most diverse mechanisms in this category, with three different types of mathematical functions and operations used (50 %). The other four mechanisms in this category only use two (33.3 %).

Table 12 shows that the logical operations, statistical function, and probability functions are the most used mathematical operation (50 %) by DDoS attack detection mechanisms based on soft-computing techniques. The algebraic function and calculus analysis are used by two of six mechanisms in this category. Meanwhile, no mechanism in this category uses the applied mathematical function. The mechanism by [24] and [26] are the most diverse in this category, with four different mathematical functions and operations (66.6 %) used. The mechanism by [25] is the least diverse (16.6 %), which only uses probability functions in their mechanism.

Table 13 shows that the use of the statistical functions is the highest at 60 %, while no mechanism in the knowledge-based category employs the calculus analysis and applied mathematical formula. The use of logical operations and algebraic functions is still low at 20 %. Meanwhile, two mechanisms by [28] and [32] are the most diverse in this category. The mechanism by [29], [30], and [31] are the least diverse as they only use one type of mathematical function and operation in their mechanisms.

Table 14 shows that four out of five (80 %) mechanisms in the clustering-based technique category use the statistical function. However, no mechanism in this category uses the logical operation and applied mathematical formula. Three mechanisms use calculus analysis (60 %), and two mechanisms use the probability function and algebraic function. The qualitative metric usage by [34] and [35] is the highest at 50 %, while the mechanism by [39] uses the least at 16.6 %.

It is evident that most researchers only employ a few mathematical operations from the list of available mathematical functions. The usage percentages for the logical, statistical, and probability functions in all twenty-two detection mechanisms are 18.2 %, 59.1 %, and 50 %, respectively. Meanwhile, only 36.4 % employ algebraic function and calculus analysis in their mechanisms. Unsurprisingly, the usage percentage of the applied mathematical function is only 4.15 percent.

The diversity of mathematical functions used in detection mechanisms and full consideration of qualitative metrics to

| Qualitative Metrics | Logical operation | Statistical function | Probability function | Algebraic function | Calculus function | Applied mathematical formula | Number of operations/
|---------------------|------------------|----------------------|---------------------|-------------------|-------------------|-----------------------------|-----------------
| Mechanisms          |                  |                      |                     |                   |                   |                             |                  |
| [33]                | 0                | 1                    | 2                   | 0                 | 0                 | 0                           | 3                |
| [33]                | 0                | 0                    | 0                   | 3                 | 0                 | 0                           | 3                |
| [34]                | 0                | 1                    | 0                   | 1                 | 3                 | 0                           | 5                |
| [35]                | 0                | 1                    | 1                   | 0                 | 1                 | 0                           | 3                |
| [36]                | 0                | 0                    | 0                   | 4                 | 0                 | 0                           | 4                |
| Number of times used| 0                | 3                    | 3                   | 4                 | 8                 | 0                           |                  |

Table 10. Quantitative metrics used for detection accuracy calculation.

| Metrics               | Description                                                                 |
|-----------------------|-----------------------------------------------------------------------------|
| True Negative (TN)    | A mechanism correctly indicates a given flow as a DDoS attack               |
| True Positive (TP)    | A mechanism correctly indicates a given flow as normal traffic              |
| False Negative (FN)   | A mechanism falsely considers normal traffic as a DDoS attack                |
| False Positive (FP)   | A mechanism falsely considers DDoS attack traffic as normal traffic.         |

VOLUME 9, 2021
123021
calculate the detection accuracy will reflect the proposed mechanism’s efficiency in terms of the reported results’ genuineness. This claim has been substantiated using the Spearman rank correlation that measures qualitative and quantitative metrics’ relationship (refer to Section 4.3.3).

2) QUANTITATIVE ANALYSIS OF DDoS ATTACK DETECTION MECHANISMS
The focus of the qualitative metrics mentioned earlier is to measure the genuineness of the detection accuracy.

This research computes the percentage of quantitative metrics usage by a mechanism using Equation (5).

\[
\text{Percentage of quantitative metrics used} = \frac{\text{number of metrics used}}{\text{Total number of metrics}} \quad (5)
\]

This research also computes the percentage of quantitative metrics usage by a mechanism using Equation (6).

\[
\text{Percentage of quantitative metrics used} = \frac{\text{number of mechanisms using quantitative metrics}}{\text{Total number of mechanisms}} \quad (6)
\]
TABLE 13. Evaluation of existing DDoS attack detection mechanisms employing knowledge-based techniques using proposed qualitative metrics.

| Mechanism | Logical Operation | Statistical Function | Probability Function | Algebraic Function | Calculus Analysis | Applied mathematical formula | Qualitative metrics in each mechanism |
|-----------|------------------|---------------------|---------------------|-------------------|------------------|-----------------------------|-------------------------------------|
| [28]      | F → 0            | T → 1               | F → 0               | T → 1             | F → 0            | F → 0                       | 2                                   | 33.3                                |
| [29]      | F → 0            | F → 0               | T → 1               | F → 0             | F → 0            | F → 0                       | 1                                   | 16.6                                |
| [30]      | F → 0            | F → 0               | T → 1               | F → 0             | F → 0            | F → 0                       | 1                                   | 16.6                                |
| [31]      | F → 0            | T → 1               | F → 0               | F → 0             | F → 0            | F → 0                       | 1                                   | 16.6                                |
| [32]      | T → 1            | T → 1               | F → 0               | F → 0             | F → 0            | F → 0                       | 2                                   | 33.3                                |
| Total     | 1                | 3                   | 2                   | 1                 | 0                | 0                           |                                     |                                     |
| Percentage of mechanism using qualitative metrics (%) | 20 | 60 | 40 | 20 | 0 | 0 |  |  |

TABLE 14. Evaluation of existing DDoS attack detection mechanisms employing clustering-based techniques using proposed qualitative metrics.

| Mechanism | Logical Operation | Statistical Function | Probability Function | Algebraic Function | Calculus Analysis | Applied mathematical formula | Qualitative metrics in each mechanism |
|-----------|------------------|---------------------|---------------------|-------------------|------------------|-----------------------------|-------------------------------------|
| [33]      | F → 0            | T → 1               | T → 1               | F → 0             | F → 0            | F → 0                       | 2                                   | 33.3                                |
| [39]      | F → 0            | F → 0               | F → 0               | F → 0             | T → 1             | F → 0                       | 1                                   | 16.6                                |
| [34]      | F → 0            | T → 1               | F → 0               | T → 1             | T → 1             | F → 0                       | 3                                   | 50                                  |
| [35]      | F → 0            | T → 1               | T → 1               | F → 0             | T → 1             | F → 0                       | 3                                   | 50                                  |
| [36]      | F → 0            | T → 1               | F → 0               | T → 1             | F → 0             | F → 0                       | 2                                   | 33.3                                |
| Total     | 0                | 4                   | 2                   | 2                 | 3                 | 0                           |                                     |                                     |
| Percentage of mechanism using qualitative metrics (%) | 0 | 80 | 40 | 40 | 60 | 0 |  |  |

The proposed quantitative metrics are used to evaluate the mechanisms discussed in Section 3. The results of the evaluation of existing DDoS attack detection mechanisms employing statistical-based techniques, soft-computing, knowledge-based methods, and clustering are shown in Table 15 to Table 18, respectively.

Table 15 shows that four mechanisms in the statistical-based technique category [20]–[22], and [23] use two out of four quantitative metrics (50%) in their detection accuracy calculation. Meanwhile, the other two [18] and [19] are not using any (0%).

Table 16 shows that the mechanism by [24] utilizes the most quantitative metrics (50%) while [37], [25], [38], and [27] are not using any (0%).

Table 17 shows that the mechanisms by [28] and [31] are the mechanisms using the quantitative metrics the most (50%), while [29], (Lu et al. [30]), and [32] are not using any (0%).

Table 18 shows that the mechanism by [39] uses the quantitative metrics the most (75%), while [34] and [36] are not using any (0%).

The study of the DDoS Attacks Detection mechanisms based on the quantitative metrics reveals several notable observations.

Most statistical technique-based mechanisms used two quantitative metrics out of four to calculate the detection accuracy, as shown in Table 15 to Table 18. Therefore, the genuineness of their accuracy calculation is only 50%. Meanwhile, some mechanisms are still at the conceptual stage, thus not using any quantitative metrics.

The average quantitative metric used by the existing mechanisms based on the statistical technique, soft computing,
knowledge, and clustering is approximately 33.3 %, 12.5 %, 20 %, and 30 %, respectively, on average.

There is a substantial lack of mathematical formulae usage in the existing detection mechanisms. Instead, researchers preferred a few elementary operations or functions from logical operations (18.2 %), statistical functions (59.1 %), and probability functions (50 %) categories, therefore adversely reduce the mechanisms’ efficacy and efficiency. The applied
mathematical functions are only found in 4.5% of the existing DDoS attack detection mechanisms reviewed.

3) STATISTICAL ANALYSIS

The third step attempts to prove the relationship between DDoS attack detection mechanisms’ accuracy and efficiency by applying the Spearman rank correlation. Applied researchers and methodologists alike widely used Spearman rank correlation to measure the strength of relationship between two sets of data. In this research, the first set of data represents the quantitative metrics while the second set of data represents the qualitative metrics. Therefore, Spearman rank correlation is a good fit to measure the relationship between the qualitative and quantitative metrics.

This step maps the quantitative metrics analysis (Table 15 to Table 18) as x-variable and the qualitative metrics (Table 11 to Table 14) as y-variable in Table 19 for twenty-two existing DDoS attack detection mechanisms.

This research measures the quantitative and qualitative metrics’ relationship of the existing mechanisms using the Spearman rank correlation (refer to Equation (7)).

\[
\text{Spearman Rank Correlation Coefficient} = 1 - \frac{6 \sum d^2}{n(n^2-1)} \tag{7}
\]

The following equation calculates the Spearman rank correlation coefficient:

\[
\text{Spearman rank correlation coefficient} = 1 - \frac{6 \sum d^2}{n(n^2-1)} = 1 - \frac{6 \times (279.5)}{10626} = 84.22\% \tag{8}
\]

Table 19 clearly shows a strong relationship between the existing quantitative metrics and the proposed qualitative metrics with a coefficient value of 84.22%. This high correlation rate reflects the genuineness of the reported DDoS attack mechanisms’ detection accuracy calculations. Considering the complement of the correlation value represents the mechanisms’ accuracy manipulation rate; therefore, the mechanisms’ accuracy manipulation rate is approximately 15.78%.

The research concludes that the lack of qualitative metrics usage in DDoS attack detection mechanisms leads to a less accurate DDoS attack detection. Similarly, a lack of qualitative metrics used in DDoS attack detection mechanisms reduces the genuineness of the calculated mechanisms’ accuracy rates.

V. RESEARCH WORKFLOW

This section summarizes the main steps to measure the qualitative and quantitative metrics’ relationship of twenty-two existing DDoS attack detection mechanisms.

1. Twenty-two DDoS attack detection mechanisms are selected and grouped according to the technique or method employed (statistical technique, knowledge-based method, soft computing, or clustering) to determine how these criteria impacted DDoS attack mechanisms’ efficiency and accuracy. Then, the mechanisms are analyzed using quantitative and qualitative metrics.

2. This research identified each mechanism’s mathematical operation and function usage and the mechanism’s gaps and drawbacks. Then, the mathematical operations and functions are grouped into six categories (logical operations, statistical functions, probability functions, algebraic functions, calculus analysis, and applied mathematical formulas), representing the qualitative metrics, as shown in Table 11 – 14.

3. The qualitative metrics, defined in Step 2, are used to measure DDoS attack detection mechanisms’ efficiency.

4. This research identified the quantitative metrics (FP, FN, TP, and TN) used by each mechanism, as shown in Table 15 – 19.

5. The quantitative metrics, defined in Step 4, are used to measure the genuineness of the DDoS attack detection mechanisms’ accuracy.

6. This research measured the qualitative and quantitative metrics’ relationship in the existing mechanisms by computing the correlation value using the Spearman rank coefficient.
TABLE 19. Calculation of spearman rank correlation coefficient.

|                      | x: Quantitative metrics | Sort (x) | Rank of x | y: Qualitative metrics | Sort (y) | Rank of y | d = x - y | d²       |
|----------------------|-------------------------|----------|-----------|------------------------|----------|-----------|-----------|----------|
| Statistical techniques| 0                       | 0        | 6         | 3                      | 1        | 4         | 2         | 4        |
|                      | 0                       | 0        | 6         | 2                      | 1        | 4         | 2         | 4        |
|                      | 2                       | 0        | 6         | 2                      | 1        | 4         | 2         | 4        |
|                      | 2                       | 0        | 6         | 3                      | 1        | 4         | 2         | 4        |
|                      | 2                       | 0        | 6         | 2                      | 1        | 4         | 2         | 4        |
|                      | 2                       | 0        | 6         | 2                      | 1        | 4         | 2         | 4        |
| Soft computing       | 2                       | 0        | 6         | 4                      | 1        | 4         | 2         | 4        |
|                      | 0                       | 0        | 6         | 1                      | 2        | 12        | -6        | 36       |
|                      | 1                       | 0        | 6         | 4                      | 2        | 12        | -6        | 36       |
|                      | 0                       | 0        | 6         | 1                      | 2        | 12        | -6        | 36       |
| Knowledge-based methods| 2                       | 1        | 12.5      | 2                      | 2        | 12        | 0.5       | 0.25     |
|                      | 0                       | 2        | 17.5      | 1                      | 2        | 12        | 5.5       | 30.25    |
|                      | 0                       | 2        | 17.5      | 1                      | 2        | 12        | 5.5       | 30.25    |
|                      | 2                       | 2        | 17.5      | 1                      | 2        | 12        | 5.5       | 30.25    |
| Clustering           | 2                       | 3        | 17.5      | 2                      | 3        | 18.5      | -1        | 1        |
|                      | 3                       | 2        | 17.5      | 1                      | 3        | 18.5      | -1        | 1        |
|                      | 0                       | 2        | 17.5      | 3                      | 3        | 18.5      | -1        | 1        |
|                      | 1                       | 2        | 17.5      | 4                      | 3        | 21        | -3.5      | 12.25    |
|                      | 0                       | 3        | 22        | 2                      | 4        | 22        | 0         | 0        |

VI. DISCUSSION

This research is the first work that combines qualitative and quantitative metrics to check the reported result’s genuineness. The proposed method is not limited to the existing mechanisms reviewed in this paper; it can also be generalized to test the manipulation or miscalculation of other types of detection mechanisms’ accuracy.

This research studied mathematical function usage in twenty-two existing DDoS attack detection mechanisms. The mathematical functions used in the existing mechanisms are classified into six categories (logical operations, statistical functions, probability functions, algebraic functions, calculus functions, and applied mathematical formula). These categories are used as qualitative metrics to measure the mathematical function’s usage level in the existing mechanisms.

This study found a lack of mathematical operation or function usage in all mechanisms’ phases, preventing high precision. Most researchers limit the use of mathematical operations that fall within the logical, statistical, or probability functions categories based on the usage percentages of 18.2 percent, 59.1 percent, and 50 percent, respectively. In comparison, the usage percentage of mathematical operations from the algebraic function and calculus analysis categories are at 36.4 percent each. Unsurprisingly, the applied mathematical function category’s usage percentage is only 4.5 percent. The existing mechanisms do not consider all quantitative metrics in calculating the detection accuracy.

The abovementioned issues related to the qualitative and quantitative metrics answered why DDoS attack issues are still not resolved despite the high detection accuracy rates of many existing DDoS attack detection mechanisms.

This research pointed out for the first time that the correlation between the quantitative and qualitative metrics in a particular mechanism reflects its efficiency; the higher the correlation value, the better the efficiency, and vice versa. We employed the Spearman rank correlation to measure the qualitative and quantitative metrics’ relationship. The high value of Spearman rank correlation (84.22) indicates a strong relationship between the quantitative and qualitative metrics for the particular mechanisms. Meanwhile, the Spearman rank correlation complement can be interpreted as representing the mechanism’s lack of efficiency. In other words, it means, based on our research finding, the percentage of the inaccuracy of the reported mechanisms’ accuracy rates is 15.78%. To eliminate the inaccurate detection rate calculation for the existing and future mathematical based DDoS flooding attack detection mechanisms, researchers must measure and calculate all four quantitative metrics and diversify the qualitative metrics in their mechanisms. Finally, it is worthwhile to mention that datasets play a significant role...
in the evaluation of DDoS detection mechanisms’ accuracy. For example, testing the detection mechanism using the same dataset used to train the detection model will increase detection mechanisms’ accuracy. But testing the detection mechanism using a different dataset than the one used to train the detection model could reduce DDoS detection mechanisms’ accuracy.

**VII. CONCLUSION**

DDoS attacks are costing many organizations significant losses in terms of financial and resources. There is also trust erosion of the users and the public at large. A comprehensive presentation of the existing DDoS detection mechanisms will provide researchers with a deep understanding and insight into the mechanisms’ nature, allowing them to improve the mechanisms’ accuracy in the future by addressing the mechanisms’ limitations.

This research pointed out the reasons for DDoS attacks’ continuous occurrences despite many highly accurate detection mechanisms by reviewing the existing DDoS attack detection mechanisms’ methods. We posit two hypotheses to explain this gap: First, weakness in the mathematical function usage by the existing mechanisms. Most mechanisms only employ a limited set of operations within the logical, statistical, or probability function categories, which affect the efficiency in terms of DDoS attack detection mechanisms’ accuracy. Second, researchers knowingly manipulate or inadvertently calculate the mechanisms’ accuracy by partially using the quantitative and qualitative metrics.

This research identified a mathematical approach (qualitative metrics) that may help researchers to improve the performance, effectiveness, and efficiency of DDoS detection mechanisms in the future. The authors believe that to enhance the DDoS attack detection mechanism’s effectiveness, the mathematical operation and function usage should extend to include a new mathematical function, such as applied mathematical functions. Applied mathematical functions have been employed in different fields and showed impressive results but are not yet widespread in network security, specifically in mathematical-based DDoS attack detection.

In the future, more mathematical-based mechanisms will be analyzed in addition to exploring different statistical analyses to measure the correlation coefficient between the qualitative and quantitative metrics. Meanwhile, this research opens the avenue for future researchers to replicate these steps for other DDoS attack detection mechanisms that use different approaches, such as deep learning or rule-based approaches.

**REFERENCES**

[1] 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., vol. 49, no. 7, pp. 24–32, Jul. 2012, doi: 10.5120/7640-0724.

[2] K. Park and H. Lee, “On the effectiveness of route-based packet filtering for distributed DoS attack prevention in power-law internets,” ACM SIGCOMM Comput. Commun. Rev., vol. 31, no. 4, pp. 15–26, 2001, doi: 10.1145/383133.383061.

[3] M. Tayab, 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, vol. 8, pp. 170529–170547, 2020, doi: 10.1109/ACCESS.2020.3022963.

[4] M. H. Bhuyan, H. J. Kashyap, D. K. Bhattacharyya, and J. K. Kalita, “Detecting distributed denial of service attacks: tools and future directions,” Comput. J., vol. 57, no. 4, pp. 537–556, 2013, doi: 10.1093/comjnl/bxt031.

[5] A. A. Bahashwian, M. Anbar, and S. M. Hanshi, Overview of IPv6 Based DDoS and DoS Attacks Detection Mechanisms, vol. 1132. Singapore: Springer, 2020.

[6] Q. Yan and F. Yu, “Distributed denial of service attacks in software-defined networking with cloud computing,” IEEE Commun. Mag., vol. 53, no. 4, pp. 52–59, Apr. 2015, doi: 10.1109/MCOM.2015.7180175.

[7] M. Darwish, A. Ouda, and L. F. Capretz, “Cloud-based DDoS attacks and defenses Marwan,” in Proc. Int. Conf. Inf. Soc. (i-Soc.), Jun. 2013, pp. 67–71.

[8] O. E. Elejla, M. Anbar, and B. Belaton, “ICMPv6-based DoS and DDoS attacks and defense mechanisms: Review,” IETE Tech. Rev., vol. 34, no. 4, pp. 390–407, Jul. 2017, doi: 10.1080/02564602.2016.1192964.

[9] S. Jin and D. S. Yeung, “A covariance analysis model for DDoS attack detection,” in Proc. IEEE Int. Conf. Commun., Jun. 2004, pp. 1882–1886, doi: 10.1109/icc.2004.1312847.

[10] O. E. Elejla, M. Anbar, and B. O. Alijla, “Flow-based IDS for ICMPv6-based DDoS attacks detection,” Arabian J. Sci. Eng., vol. 43, no. 12, pp. 7757–7775, Dec. 2018, doi: 10.1007/s13369-018-4314-9.

[11] O. E. Elejla, B. Belaton, M. Anbar, B. Alabsi, and A. K. Al-Ani, “Comparison of classification algorithms on ICMPv6-based DDoS attacks detection,” in Computational Science and Technology (Lecture Notes in Electrical Engineering), vol. 481. Singapore: Springer, Aug. 2018, pp. 347–357, doi: 10.1007/978-981-13-2622-6_34.

[12] J. Mirkovic and P. Reihier, “A taxonomy of DDoS attack and DDoS defense mechanisms,” ACM SIGCOMM Comput. Commun. Rev., vol. 34, no. 2, pp. 39–53, Apr. 2004, doi: 10.1145/997150.997156.

[13] O. E. Elejla, M. Anbar, B. Belaton, and S. Hamouda, “Labeled flow-based detection of ICMPv6 attacks,” Neural Comput. Appl., vol. 31, no. 8, pp. 3629–3646, Aug. 2019, doi: 10.1007/s00521-017-3319-7.

[14] A. K. Al-Ani, M. Anbar, S. Manickam, and A. Al-Ani, “DAD-match; Security technique to prevent denial of service attack on duplicate address detection process in IPv6 link-local network,” PLoS ONE, vol. 14, no. 4, pp. 1–20, 2019, doi: 10.1371/journal.pone.0214518.

[15] A. K. Al-Ani, M. Anbar, A. Al-Ani, and D. R. Ibrahim, “Match-prevention technique against distributed denial of service attacks over multiple network domains,” in Proc. Int. Conf. Intell. Transp. Syst. (ITSC), Nov. 2018, pp. 157–163, doi: 10.1109/ITSC.2018.8569698.

[16] K. J. Singh and T. De, “Mathematical modelling of DDoS attack and detection using correlation,” J. Cyber Secur. Technol., vol. 1, nos. 3–4, pp. 175–186, Oct. 2017, doi: 10.27429/jcst.2017.1384213.

[17] M. H. Bhuyan, D. K. Bhattacharyya, and J. K. Kalita, “An empirical evaluation of information metrics for low-rate and high-rate DDoS attacks detection,” Pattern Recognit. Lett., vol. 51, pp. 1–7, Jan. 2015, doi: 10.1016/j.patrec.2014.07.019.

[18] P. Shamsolmoali and M. Zareapoor, “Statistical-based filtering system against DDOS attacks in cloud computing,” in Proc. Int. Conf. Adv. Comput., Commun. Informat. (ICACCI), Sep. 2014, pp. 1234–1239, doi: 10.1109/ICACCI.2014.6968282.

[19] G. Zhang, S. Jiang, G. Wei, and Q. Guan, “A prediction-based detection technique against distributed denial-of-service attack on address resolution protocol,” Comput. Sci. J., vol. 15, pp. 488–504, Jun. 2009, doi: 10.1109/1582379.1582403.

[20] C.-L. Chen, “A new detection method for distributed denial-of-service attack traffic based on statistical test,” J. Univers. Comput. Sci., vol. 15, no. 2, pp. 488–504, 2009.

[21] Y. Chen, K. Hwang, and W. S. Ku, “Collaborative detection of DDoS attacks over multiple network domains,” IEEE Trans. Parallel Distrib. Syst., vol. 18, no. 12, pp. 1649–1662, Dec. 2007, doi: 10.1109/TPDS.2007.1111.
L. Limwiwatkul and A. Rungsawang, “Distributed denial of service detection system in software-defined networking (SDN),” *ICTS Trans. Secur. Saf.*, vol. 4, no. 12, Dec. 2017, Art. no. 153515, doi: 10.4108/eai.28-12.2017.153515.

J. Choi, C. Choi, B. Ko, and P. Kim, “A method of DDoS attack detection using HTTP packet pattern and rule engine in cloud computing environment,” *Soft Comput.*, vol. 18, no. 9, pp. 1697–1703, Sep. 2014, doi: 10.1007/s00500-014-1250-8.

H. V. Nguyen and Y. Choi, “Proactive detection of DDoS attacks utilizing k-NN classifier in an anti-DDoS framework,” *Int. J. Electr. Comput. Eng.*, vol. 4, no. 4, pp. 247–252, Feb. 2010.

D. Gavrilis and E. Dermatas, “Real-time detection of distributed denial-of-service attacks using RBF networks and statistical features,” *Comput. Netw.*, vol. 48, no. 2, pp. 235–245, Jun. 2005, doi: 10.1016/j.comnet.2004.08.014.

M. Elgendi, “Fast QRS detection with an optimized knowledge-based method: Evaluation on 11 standard ECG databases,” *PLoS ONE*, vol. 8, no. 9, Sep. 2013, Art. no. e73557, doi: 10.1371/journal.pone.0073557.

A. S. SyedNavaz, V. Sangeetha, and C. Prabhadevi, “Entropy based anomaly detection system to prevent DDoS attacks in cloud,” *Int. J. Comput. Appl.*, vol. 62, no. 15, pp. 42–47, Jan. 2013, doi: 10.5120/10160-5084.

K. Lu, D. Wu, J. Fan, S. Todorovic, and A. Nucci, “Robust and efficient detection of DDoS attacks for large-scale internet,” *Comput. Netw.*, vol. 51, no. 18, pp. 5036–5056, Dec. 2007, doi: 10.1016/j.comnet.2007.08.008.

L. Limwiwatkul and A. Rungsawang, “Distributed denial of service detection using TCP/IP header and traffic measurement analysis,” in *Proc. IEEE Int. Symp. Commun. Inf. Technol.*, vol. 1, Oct. 2004, pp. 605–610, doi: 10.1109/ISICT.2004.1412917.

R. Thomas, H. Zhu, T. Huck, and T. Johnson, “NetBouncer: Client-legitimacy-based high-performance DDoS filtering,” in *Proc. DARPA Inf. Survivability Conf. Expo.*, Apr. 2003, p. 111, doi: 10.1109/DISCEX.2003.1194939.

X. Qin, T. Xu, and C. Wang, “DDoS attack detection using flow entropy and clustering technique,” in *Proc. 11th Int. Conf. Comput. Intell. Secur. (CIS)*, Dec. 2015, pp. 412–415, doi: 10.1109/CIS.2015.105.

M. Li and M. Li, “A new approach for detecting DDoS attacks based on wavelet analysis,” in *Proc. 2nd Int. Congs. Image Signal Process.,* Oct. 2009, pp. 1–5, doi: 10.1109/CISP.2009.5309903.

K. Lee, J. Kim, K. H. Kwon, Y. Han, and S. Kim, “DDoS attack detection method using cluster analysis,” *Expert Syst. Appl.*, vol. 34, no. 3, pp. 1659–1665, Apr. 2008, doi: 10.1016/j.eswa.2007.01.040.

L. Li and G. Lee, “DDoS attack detection and wavelets,” *Telecommun. Syst.*, vol. 28, nos. 3–4, pp. 435–451, 2005, doi: 10.1007/s11235-004-5581-0.

Y. Purwanto and B. Rahardjo, “Traffic anomaly detection in DDoS flooding attack,” in *Proc. 8th Int. Conf. Telecommun. Syst. Services Appl. (TSSA)*, Oct. 2014, pp. 1–6, doi: 10.1109/TSSA.2014.7065953.

R. Jalili, F. Inani-Mehr, M. Amini, and H. R. Shahriari, “Detection of distributed denial of service attacks using statistical pre-processor and unsupervised neural networks,” in *Proc. 1st Int. Conf. Inf. Secur. Pract. Exp. (ISPEC)*, vol. 3439, Apr. 2005, pp. 192–203, doi: 10.1007/3-540-31979-5_17.

Q. Liao, H. Li, S. Kang, and C. Liu, “Application layer DDoS attack detection using cluster with label based on sparse vector decomposition and rhythm matching,” *Secur. Commun. Netw.*, vol. 5, pp. 422–437, Jun. 2015, doi: 10.1002/sec.1236.

I. Goni and A. Lawal, “A propose neuro-fuzzy-genetic intrusion detection system,” *Int. J. Comput. Appl.*, vol. 115, no. 8, pp. 5–9, Apr. 2015.

H. M. Bhuyana, D. K. Bhattacharyyab, and J. K. Kalitat, *An Empirical Evaluation of Information Metrics for Low-Rate and High-Rate DDoS Attack Detection*. Amsterdam, The Netherlands: Elsevier, 2015.