Indonesian Journal of Electrical Engineering and Computer Science
Vol. 14, No. 1, April 2019, pp. 155~168
ISSN: 2502-4752, DOI: 10.11591/ijeecs.v14.i1.pp155-168

Systematic review of aspects of DDoS attacks detection

Silvia Bravo[1], David Mauricio[2]
[1]Faculty of Engineering and Applied Sciences, Technical University of Cotopaxi, Latacunga, Ecuador
[2]Department of Computer Science, National University of San Marcos, Lima, Peru

Article Info

Article history:

Received Jul 7, 2018
Revised Oct 10, 2018
Accepted Nov 25, 2018

Keywords:

Attack detection
DDoS
Distributed denial of service

ABSTRACT

Distributed Denial of Service attacks (DDoS) are one of the biggest problems facing the Internet. To eliminate this type of attack, the number of which has increased in the period under study, various methods of defense have been proposed. However a detection mechanism that is able to completely counteract the attacks has not yet been found. Therefore, detection and defense against DDoS attacks is of great importance for specialists engaged in computer security. This paper presents a systematic review of the scientific literature on methods of detecting DDoS attacks. From the literature the main aspects related to detection have been formulated. Six aspects for analysis in this investigation were identified: techniques, variables, tools, deployment location, point in time and detection accuracy. It was found that each technique used for the detection of attacks exploits certain characteristics of the network traffic, user requests and specific tools. Finally, it managed to identify the mechanisms that have the highest detection accuracy, such as the datasets they use. It has been concluded that an adequate analysis of the above aspects of detection of DDoS attacks can make a useful contribution to designing an appropriate strategy for neutralizing the attacks.

Corresponding Author:

Silvia Bravo,
Faculty of Engineering and Applied Sciences,
Technical University of Cotopaxi,
Latacunga 050150, Ecuador.
Email: silvia.bravom@utc.edu.ec

1. INTRODUCTION

Computer attacks, such as denial of service (DoS), are a threat to Internet security and have posed a problem since its appearance in 1980 [1]. These attacks are illegal actions through which an attacker interrupts the resources or services of a system [2] and affects access to the network, online accounts, email and computer resources [3].

Later, a more sophisticated type of DoS attack called Distributed Denial of Service (DDoS) appeared. This attack involves two or more computers, which can be located in different parts of the world, and are executed by the same attacker [4]. The first reports of this type of attack appeared in 1999 [5]. In [6] they states that the main problem to detect this type of attack is to differentiate the legitimate flows from the attack flows, which results in high rates of false positives and negatives in the detection methods used. Therefore, the research topic of detection of DDoS attack has generated great interest in the scientific community. Likewise, [7] they suggest a classification of this type of attacks, according to the layer in which they are executed, these are network layer and application layer.

Several investigations focus their efforts on the review of aspects that intervene in the detection of DDoS attacks. In [7] they conducted an review of the literature on attacks and defense mechanisms with an analysis of prevention, detection and response. On the other hand, [8] they published a review article describing the characteristics of the mechanisms by means of which the network detection mechanism and

the reaction to an attack are activated. In [9] they presented an investigation of DDoS attacks, detection methods and tools used in wired networks. Although these works analyze the detection mechanisms, they are limited to an analysis at the network layer level and the depth application layer is not considered where the attacks have a considerable impact in recent years, such as show several studies [10]-[12]. In addition, these works do not consider the aspects that characterize the detection of DDoS attacks for a possible improvement of it.

Therefore, this paper presents the aspects that characterize the detection of DDoS attacks, these aspects are techniques, variables and tools used, as well as where the detection was implemented and at what point in time. For the aforementioned, the main objective of this document is to carry out a systematic review of the literature to analyze these aspects of detection of DDoS attacks. For this, six research questions have been raised and presented in Section 2. These questions have helped to identify, evaluate and interpret the main relevant issues related to the topic. The present work is organized according to the following structure. In Section 2 explains the methodology used. Section 3 performs an analysis and discussion of the results. Finally, Section 4 presents the conclusions drawn from this study.

2. RESEARCH METHOD

The systematic review for carrying out this research is based on the model proposed by [13], which is divided into three phases:

Planning the review: questions are raised as to the goals of the research and review.

Conducting the review: in this stage the plan is executed and major studies following the inclusion and exclusion criteria selected are referred to or discarded.

Reporting the review: at this stage the results of the statistical review and analysis presented in sections III, are shown.

2.1. Planning the review

To carry out the literature review on the detection of DDoS attacks the following research questions were raised:

Q1: What are the techniques used for detection?

Q2: What are the variables used?

Q3: What are the tools used?

Q4: Where are they implemented?

Q5: At what point in time before the attacks must the detection mechanism be activated?

Q6: With what ratio of precision do the techniques detect a DDoS attack?

Answers to the above research questions, were found in the following data sources: DOAJ (Directory of Open Access Journal), IEEE Xplore, Science Direct and Springer. To find scientific articles published in journals with an impact factor of SJR (Scimago Journal and Country Rank), in the period between 2005 to 2017, the following search procedure was undertaken, as shown in Table 1, taking into account the title, abstract and keywords.

In addition, these terms are adapted to match the research questions and individual needs of the search engine. To the results of searches from various sources of information the criteria for inclusion and exclusion shown in Table 2 were applied.

Table 1. Source String

Source	String
DOAJ	distributed denial of service or ddos; 2005-2017
IEEE Xplore	((distributed denial of service) OR ddos) and refined by Year: 2005-2017
Science Direct	pub-date ¿= 2005 and (distributed denial of service) and ddos
Springer	”distributed denial of service” or ”ddos”’within 2005 - 2017

Table 2. Inclusion and exclusion criteria

Inclusion criteria	Exclusion criteria
Models, methods and techniques for detecting DDoS attacks	Detection submits proposals that do not include the experimental results
Proposed variables in the detection attacks	Present detection mechanisms in general botnets
Proposed components that make up the mechanism	Books, proceedings, posters, theses, workshops
Proposed tools in the detection mechanisms	Presented in its tracking attack flow
Directly answer the research questions	Submit contributions that aim to cloud computing environments, P2P networks, MANET, wireless local areas, data centers, high speed networks and DNS servers

2.2. Conducting the review

The search results obtained, according to the proposed strategy, were subjected to a selection process, according to the inclusion and exclusion criteria established. It was necessary to make a preliminary review of their content in order to determine their relevance to the present study and to determine whether these works apply to the detection of DDoS attacks. Most of the items were discarded because they corresponded to another subject under study, such as surveys, taxonomy and botnets. The process implemented and the results obtained at each stage are shown in Figure 1. Subsequently, we proceeded to analyze the articles in order to answer the research questions.

The results of the search performed showed a total of 1341 articles. Of these, 81 were selected, that met the inclusion and exclusion criteria established, as can be seen in Table 3.

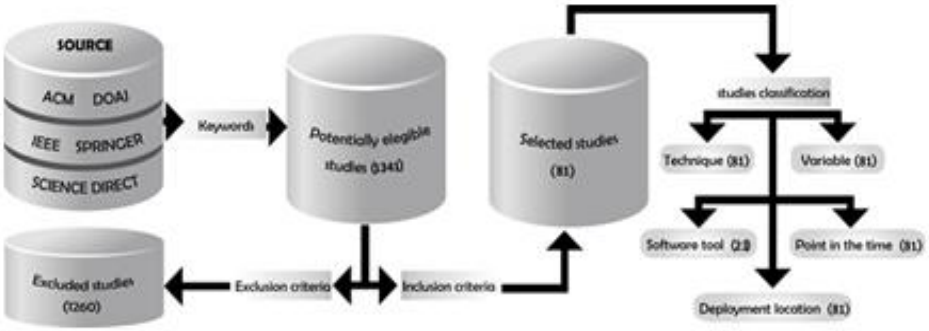

Figure 1. Process for exploring the literature

Table 3. Selected articles

Source	Potentially eligible studies	Selected studies (Journal article)
DOAJ	158	20
IEEE Xplore	80	21
Science Direct	843	30
Springer	260	10
Total	1341	81

2.3. Time trends of the publications

Figure 2 shows the temporal trend of the publications on the detection of DDoS attacks, selected from the methodology, by phase conducting the review sample. In it, you can see the increase in the number of publications over the past 13 years can be seen. The trend in the number of published papers reflects the importance that has been given to this subject of study by the scientific community.

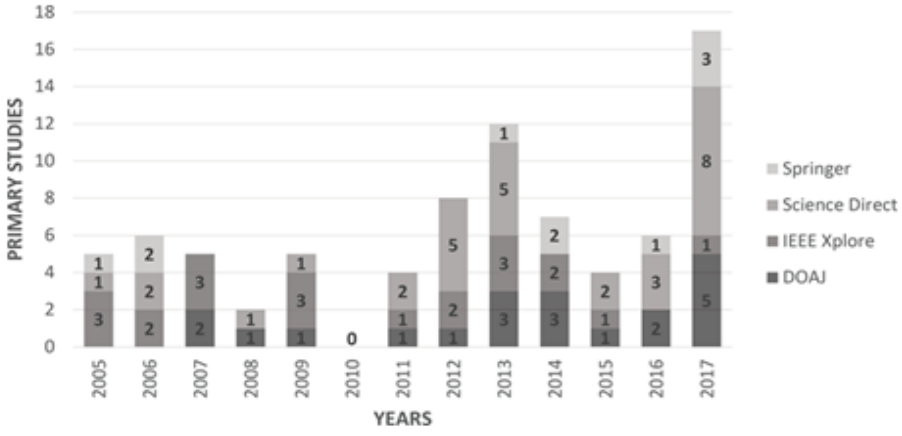

Figure 2. Time trend of publications on DDoS attack detection

2.4. Data Sources

The search results show that the largest number of articles were obtained from the Science Direct databases and IEEE Xplore. Moreover, reference sources that provided some information on the subject were Springer and DOAJ, as can be seen in Table 3.

2.5. Aspects

The following items on the detection of DDoS attacks were chosen: techniques, variables, tools, deployment location, point in time and detection accuracy. Table 4 shows these aspects together with their respective definitions:

Table 4. Definitions of aspects

Aspects	Definition
Technique	It refers to the set of procedures or resources used in a particular activity. In this paper we consider the techniques employed by detection mechanisms.
Variable	It is defined as the character that is measured in different individuals or objects. In this study it responds to the need to know the features used the mechanism for detecting DDoS attacks.
Software tools	These are computer programs that help the specialist in the design process and the development of software or documentation [14].
Deployment location	It refers to the location were the detection mechanism should be deployed i.e., at the source, in the network, at the destination or a hybrid of the above.
Point in time	It is defined as the moment when the detection mechanism should be activated i.e., before, during or after the attack.
Accuracy/Detection Rate	The overall value of all correctly classified instances i.e., both true positives and true negatives [15]

Table 5 shows the distribution of the 81 selected studies, in accordance with the aspects identified for detecting DDoS attacks as defined above. It can be seen that 100% of the selected papers presented at least one technique fo|r detecting attacks. Also, only 28% mention the tool used to implement the technique for detecting a DDoS attack.

Table 5. Aspects of DDoS attacks detection

Source	Technique	Variable	Tools	Deployment location	Point in time
DOAJ	[16] [17] [18] [19] [20] [21] [22] [23] [24] [25] [26] [27] [28] [29] [30] [31] [32] [33] [34] [35]	[16] [17] [18] [19] [20] [21] [22] [23] [24] [25] [26] [27] [28] [29] [30] [31] [32] [33] [34] [35]	[16] [17] [23] [26] [32] [35]	[16] [17] [18] [19] [20] [21] [22] [23] [24] [25] [26] [27] [28] [29] [30] [31] [32] [33] [34] [35]	[16] [17] [18] [19] [20] [21] [22] [23] [24] [25] [26] [27] [28] [29] [30] [31] [32] [33] [34] [35]
IEEE Xplore	[36] [37] [38] [39] [40] [41] [42] [43] [44] [45] [46] [47] [48] [49] [50] [51] [52] [53] [54] [55] [56]	[36] [37] [38] [39] [40] [41] [42] [43] [44] [45] [46] [47] [48] [49] [50] [51] [52] [53] [54] [55] [56]	[38] [46]	[36] [37] [38] [39] [40] [41] [42] [43] [44] [45] [46] [47] [48] [49] [50] [51] [52] [53] [54] [55] [56]	[36] [37] [38] [39] [40] [41] [42] [43] [44] [45] [46] [47] [48] [49] [50] [51] [52] [53] [54] [55] [56]
Science Direct	[57] [58] [59] [60] [61] [62] [63] [64] [65] [66] [67] [68] [69] [70] [71] [72] [73] [74] [75] [76] [77] [78] [79] [80] [81] [82] [83] [84] [85] [86]	[57] [58] [59] [60] [61] [62] [63] [64] [65] [66] [67] [68] [69] [70] [71] [72] [73] [74] [75] [76] [77] [78] [79] [80] [81] [82] [83] [84] [85] [86]	[59] [60] [61] [62] [63] [68] [70] [71] [72] [73] [74] [82] [86]	[57] [58] [59] [60] [61] [62] [63] [64] [65] [66] [67] [68] [69] [70] [71] [72] [73] [74] [75] [76] [77] [78] [79] [80] [81] [82] [83] [84] [85] [86]	[57] [58] [59] [60] [61] [62] [63] [64] [65] [66] [67] [68] [69] [70] [71] [72] [73] [74] [75] [76] [77] [78] [79] [80] [81] [82] [83] [84] [85] [86]
Springer	[87] [88] [89] [90] [91] [92] [93] [94] [95] [96]	[87] [88] [89] [90] [91] [92] [93] [94] [95] [96]	[92] [96]	[87] [88] [89] [90] [91] [92] [93] [94] [95] [96]	[87] [88] [89] [90] [91] [92] [93] [94] [95] [96]
Total	81	81	23	81	81

3. RESULTS AND DISCUSSION

The analysis of the information collected in Section 3 was performed on the basis of the research questions posed in Section 2. The results are presented in tables containing the description of the aspect to be analyzed, together with the names of the authors who used them.

3.1. Q1: What are the techniques used in the detection?

The techniques used in the detecting DDoS attacks are shown and described in Table 6. As can be appreciated in this table different techniques 48 have been proposed. The aspects of each technique are discussed in Table 6.

Table 6. Techniques used for detecting DDoS attacks

Id	Technique	Description
T1	Bagging	Representative of parallel ensemble learning methods. It employs Random Sampling in sampling data set.The algorithm focuses mainly on decreasing variance.
T2	Bat Algorithm	The bat algorithm uses the echo based location determining behavior of bats to solve both single objective and multi-objective optimization problems.
T3	Bloom filter	The Bloom filter is a kind of space-efficient hash data structure. We propose using a modified Bloom filter in order to construct a hash table that can record three-way TCP control packets at a limited storage cost.
T4	Change aggregation tree (CAT)	This CAT mechanism is designed for use at the router level for detecting abrupt changes in traffic flows.When a DDoS attack is launched, the routers observe changes in the space temporal distribution of traffic volumes.
T5	Cluster analysis	Cluster analysis is to group data so that objects in a given group are similar to each other and dissimilar from to those in other groups. By using cluster analysis, we can separate normal traffic and each phase of the DDoS forming clusters have dissimilarities among them attack into partitioned groups if the variables involved in
T6	Congestion Participation Rate (CPR)	Congestion Participation Rate (CPR) to identify LDDoS flows by measuring the intention of network flows to congest the network. To the best of our knowledge, it is the first metric that is able to recognize LDDoS flows by quantifying each flowjs intention to congest the network.
T7	Correlation analysis	The correlation is used to describe the similarity of different flows. However, in some cases, it may indicate zero correlation. Although the two flows are completely correlated there is a phase difference.
T8	Counter mechanism	Assigns a continuous value as opposed to a binary measure to each client session, and the scheduler utilizes these values to determine if and when to schedule a sessionjs requests.
T9	Cuckoo search	Technique stimulated by the parasite act of some Cuckoo birds. The species of type Cuckoo unable to complete its reproduction cycle without proper host.
T10	Cusum algorithm	A nonparametric cumulative sum (CUSUM) procedure commonly used for detection of wide range of possible shifts and is generally favored for its simplicity and low computational overhead.
T11	Entropy	Renyi's generalized entropies is a family of measures that characterize the distribution of a random variable. Shannon entropy has been used to conceptualize source address entropy and traffic cluster entropy.
T12	Firewall	Firewall function as above, giving the defender the option to set the value which is the threshold above which all the packets of a flow are dropped.
T13	Fuzzy logic	Fuzzy estimator on the mean packet between arrival times. It interprets the rules well but it suffers from the disadvantage of not being able to acquire the rules automatically.
T14	Genetic algorithms	A Genetic algorithm is a heuristic search that mimics the process of natural evolution. Genetic algorithms belong to the larger class of evolutionary algorithms (EA), which generate solutions to optimization problems using inheritance, mutation, selection, and crossover techniques inspired by natural evolution, such as
T15	Googles strategic position	The main idea of JUST-Google is to let ISPs edge routers allow traffic originating from sources that are approved by Google and destined to a victim within that ISP to pass while filtering all other traffic destined to the same victim. An HsMM algorithm that describes the stochastic process varying with time and monitors the App-DDoS attacks occurring during a flash crowd event.
T16	Hidden semi-Markov model (HsMM)	An HsMM algorithm that describes the stochastic process varying with time and monitors the App-DDoS attacks occurring during a flash crowd event.
T17	Hop-Count Filtering	The source IP address serves as the index in the table for retrieving the correct hop-count for this IP address. If the computed hop-count matches the stored hop-count, the packet has been authenticated.
T18	Information distance	A metric used to detect low-rate DDoS attacks by measuring the difference between legitimate traffic and attack traffic.
T19	Information divergence	Estimates the distances between the probability measurements independently of the parameters and detects the attacker and discards the adversarys packets for a fixed amount of time in an organized manner.
T20	Joint Deviation Rate (JDR)	Joint Deviation Rate (JDR), a new metric to describe the deviation rate of the network traffic states. JDR is a combination of the deviations of all the multiple features in Network Traffic State (NTS).
T21	K-nearest neighbors	The k-nearest neighbor algorithm is a method that predicts flow classes based on the k-closest training examples in feature space. A flow is classified by the majority vote of its neighbors and k is a positive integer, typically small.
T22	Kolmogorov Complexity	Kolmogorov Complexity states that the joint complexity measure of random strings is lower than the sum of the complexities of the individual strings when the strings exhibit some correlation.

Id	Technique	Description
T23	Mapping Service	A service provider registers the binding(s) from its domain name(s) to the IP addresses into the domain name system (DNS). When a customer wants to obtain a service from the service provider, his/her computer first queries domain name and then sends a request to the server that uses the returned IP address.the IP address corresponding to the service providerjs
T24	Mathematical model	Mathematical model for estimating the attack effect of this stealthy type of DDoS. By originally capturing the adjustment behavior of a victim in the TCP congestion window, our model can comprehensively evaluate the configured) and the affect of the attack on the network environment.combined impact of the attack pattern (i.e., how the attack is
T25	Multi-agent application	An agent is built as an aggregation of capabilities, and such capabilities are selected according to the primitive actions that a mechanism provides.
T26	Neural Network	A Neural network consists of processing elements called neurons. These neural networks are designed to learn a new pattern, new association, and new functional dependencies. The advantage of a neural network is a better generalization capability.
T27	Neyman Pearson cost minimization strategy	Neyman Pearson (NeP) theory where prior knowledge of the distribution of data is not known. The NeP hypothesis is useful in situations where different types of error have different consequences.
T28	Overlay network	Maintains virtual rings or shields of protection around registered customers. A ring is composed of a set of IPSs that are at the same distance (number of hops) from the customer.
T29	Packet filtering	Packet classification and filtering scheme to be implemented at the edge routers of the ISP network that contains the targeted system, and should be activated after a TCP-based reflector DDoS attack has been detected.
T30	Packet marking	A scheme that allows a DDoS victim to filter out attack packets on a per packet basis with a high accuracy after only a few attack packets have been received.
T31	Path identifiers	Used in negotiated between neighboring domains as interdomain routing objects.
T32	Pushback	Commands can contain some rate-limit requests, so that, when an upstream router receives the command, it will rate-limit the traffic to the victim and not cause congestion near the victim.
T33	Puzzle Solving	Captures complex temporal correlations across multiple time scales with very low computational complexity.
T34	Queuing model	Carries information about traffic characteristics and congestion properties.
T35	Random Forrest	Random Feature Selection is farther introduced in the training process for Random Forest.
T36	Rate-limit filters	The congested router starts with a local rate limit, and then progressively pushes the rate limit to some neighbor routers and further out, forming a dynamic rate-limit tree, which can be expensive to maintain.
T37	Ratio of Collective Flow (RCF)	Responsible for classifying a flow as legitimate, suspicious or attack flow based on the basis of packet information obtained from the monitoring module and the current load on an outgoing queue.
T38	Resilient Back Propagation (RBP)	The RBP algorithm was found to perform better. A single classifier commits errors on different training samples. So, by creating an ensemble of classifiers and combining their outputs, the total error can be reduced and the detection accuracy can be increased.
T39	Router throttling	Contributes to the fundamental understanding of router throttling as a mechanism against DDoS attacks. In particular, a control-theoretical model useful for understanding a system is behavior under a variety of parameters and operating conditions.
T40	Routing Information Protocol (RIP)	RIP (routing information protocol), a representative protocol of IGP (interior gateway protocol). RIP, which works by the exchange of tables among routers, operates inside AS (an autonomous system). RIP is used as the routing protocol on the inside of AS.
T41	Semantic traffic differentiation	Semantic traffic differentiation has two main advantages over per packet and per-user differentiation approaches: 1) It easily spots randomly generated attack traffic (with or without spoofing) since such traffic creates short-lived structures with no higher semantics. 2) It easily spots structures that are engaged in one-way communications, aggressively sending traffic to an unresponsive party.
T42	Signature based	Profiles which describe of characteristics of a known network security according to the security requirements of network objects on a network.
T43	Special Sequence Matrix	SSM is a dynamic spanning matrix. Used in bModel they are produced dynamically and cause the diameter of the matrix to grow dynamically as well.
T44	Spectral analysis	Spectra analysis can be applied to both training traffic and the incoming traffic streams to the tesbed. Leveraging spectral analysis, our hypothesis testing model make spectral template matching effective by detecting shrew DDoS attacks at traffic streaming level and by cutting off malicious flows at a refined flow level.
T45	Statistical Methods	The key idea is to prioritize a packet based on a score which estimates its legitimacy given the attribute values it carries.
T46	Support-vector data description (SVDD)	An anomaly-detection method that uses unlabeled data to find a model for unusual instances.
T47	TCP/IP and HTTP statistics	The following statistical values are computed for each incoming user: number of get requests, standard deviation of get, mean of flows per user, standard deviation of flows per user and standard deviation of posts, flows per minute per user, request per minute per user and so on.
T48	Wavelet Analysis	Captures a complex temporal correlation across multiple time scales with a very low computational complexity.

Table 6 shows the results of 81 studies that present DDoS attack detection techniques. While in Table 8, it can be seen that the Neural Network technique is used more frequently, having been applied in eight studies. Therefore, it is evident that this technique is the most commonly used due to its computational and logical capacity to identify anomalies between data flow entries. Entropy is used by 6 attack detection studies. This technique is used because it allows identifying certain characteristics of a data flow that would allow the detection of a DDoS attack. It can be concluded that the most commonly used techniques analyze the data flow for the detection of DDoS attacks and focus on the network layer.

3.2. Q2: What are the variables used in the detection?

In the studies analyzed a total of 28 variables for the detection of DDoS attacks were identified, as can be seen in Table 7. This table also provides a description of the variables that have been identified.

Table 7. Variables used by DDoS attack detection techniques

Id	Variable	Description
V1	Absolute bandwidth consumption	This feature represents the average bandwidth consumed by the requests found in absolute time interval defined. This feature also considered as significant since the estimation of bandwidth consumption is critical in load assessment.
V2	Absolute page access count	This feature represents the average number of requests in an absolute time interval defined. This feature also critical one among the considered features, since the page access count along with absolute session interval optimizes the detection of the load on target web server.
V3	Absolute page access time	This feature represents the average time spent on each page request in an absolute time interval defined. The motive to consider this feature is, load of requests with minimal access time of each page is suspicious.
V4	Absolute session count	This feature represents the average number of sessions found in an absolute time interval defined. This feature is considered since the load on any target web server estimated by the number of sessions in a given time interval.
V5	Absolute session interval	This feature represents the average time render each session in an absolute time interval defined. This feature is critical as the session time indicates the time spent by a source on the target web server with an intension of fair use or an attack.
V6	Absolute time interval	This denotes the absolute time taken by the set of sessions initiated at given threshold time frame. This feature considered as significant, as HTTP-flood is cumulative of multiple sessions and diversified packet flow. The features explored further for defined absolute time interval.
V7	ACK number	ACK number sent by the receiving terminal is the last Sequence Number when communication was successful.
V8	Click rates of web objects	Estimation of the click-through rate of available ads for a given search query. The more interactive it is, the higher the click-through rate is.
V9	Eminent source diversity ratio	This feature represents the average number of divergent sources those initiate the sessions in an absolute time interval defined. The request load from eminent sources is tolerable, hence this feature considered as significant.
V10	IP address	The only valid IP source address for packets originating from the PC is the one assigned by the ISP (whether statically or dynamically assigned).
V11	Network traffic	Remote logins and file transfers
V12	Number of connections	Behavioral characteristics of a connection in terms of number, type of various data items with respect to time. These features are used to determine the statistical properties, such as standard deviation and variance.
V13	Number of ICMP	Number of ICMP echo reply packets from the same source.
V14	Number of packets	Packets transmitted or received without errors.
V15	Number of requests	Requests for currently open windows and whether the number of requests for an open window of time is viable.
V16	Number of UDP	Number of UDP echo packets to a specified port
V17	Number of users	Set of real users accessing a server
V18	Packets	Packets carrying path information. The victim node can defend itself from DDoS attack by filtering the packets transmitting via/from an attacking node.
V19	Port	The I/O port determines which service ports are being used.
V20	Protocol	Internet Protocols (IP), there is now a standard for how general purpose computers, such as personal computers, workstations and servers can interchange data over the telephone system.
V21	Rate of packets	This feature is calculated on the packets sent from a particular sender.
V22	Ratio of incoming SMTP packets	A host that does not have any incoming connection is more likely to be a spammer than one that has incoming SMTP traffic
V23	Ratio of outgoing SMTP packets	Shows the outgoing SMTP traffic time series for a host known to have sent spam
V24	Session‘s requests	Session inter-arrival times between consecutive sessions
V25	TCP flows	Flows with a large amount of data to send, such as FTP transfers
V26	Traffic rate	Defined as the total number of bits received over a certain time interval.
V27	Type of packet	Fundamentally, all networks have essentially two kinds of packets. Data packets that belong to users and carry users or application traffic. Control packets belong to the network and are used to dynamically build and operate the network
V28	Variance of time	Variance of time difference between two consecutive packets

Table 8 shows the variables used by the detection techniques and the authors who used the mentioned techniques are summarized. It can be seen that the most commonly used variables are packets and IP addresses. The packages are used for detection because they contain data such as IP source, weight, speed, among others. While the IP address is used to identify the origin of the data flow, which allows to cut the traffic that is sent from them when it is identified as an attack. It is important to note that these variables are used in mechanisms that correspond to the detection of DDoS attacks in the network layer.

Table 8. Techniques, studies and variables used by the detection mechanisms of DDoS attacks

Technique	V1	V2	V3	V4	V5	V6	V7	V8	V9	V10	V11	V12	V13	V14	V15	V16	V17	V18	V19	V20	V21	V22	V23	V24	V25	V26	V27	V28
T1											[34]														[34]			
T2		[81]			[81]	[81]											[81]	[81]										
T3																		[89]										
T4										[41]									[41]	[41]								
T5										[60] [32]				[60]					[60]								[60]	
T6											[68]																	
T7										[86]				[49]	[92]										[86]			
T8										[20] [24] [47]								[20]						[45]				
T9	[83] [94]	[94]	[83] [94]	[83] [94]	[83] [94]	[83] [94]			[84] [94]																			
T10						[79]						[79]			[79]						[79]							
T11					[77]					[47] [28] [77]	[19]							[26] [84]										
T12										[18]								[72] [90]										
T13						[69]						[70]	[70]			[70]						[70]	[70]					[70]
T14										[64] [29] [85]		[70]	[70]		[85]	[70]			[85]	[85]		[70]	[70]					[70]
T15										[22]																		
T16								[25]							[46]		[46]											
T17										[43]																		
T18										[54]	[30]							[31]										
T19										[65] [95]				[73]														
T20										[67]								[67]	[67]	[67]					[67]			
T21																		[74] [34] [88]							[34]			
T22																												
T23										[51]				[51]														
T24																									[53]			
T25										[82]																		
T26										[29] [35] [78] [85]	[50] [52]	[70]	[70]	[44]		[70]		[78]	[85] [78]	[35] [85]	[35]	[70]	[70]	[85]				[70]
T27											[63]																	
T28															[48]													
T29							[58]			[57] [58]								[17] [27] [71]										
T30																		[16] [40] [42] [71]										
T31										[56]																		
T32																		[42]										
T33																								[55]				
T34										[62]								[61]										
T35																		[34]							[34]			
T36																		[36]										
T37																		[21]										
T38											[63]																	
T39																		[75]								[38]		
T40												[91]																
T41										[37]																		
T42										[23] [96]	[30]								[23] [96]	[23]								
T43															[92]													
T44										[59]									[59]	[59]								
T45										[33] [76]								[39] [76]	[76]	[76]					[76]			
T46												[93]						[93]		[93]								
T47						[69]								[69]	[69]													
T48											[87]																	

3.3. What are the tools used to implement the techniques?

The ten tools used for the implementation of detection techniques are shown in Table 9. The same evidence shows that the two most commonly used tools are Matlab and the Network simulator. This is due to the fact that these two tools present functionalities for the adequate implementation of the detection mechanisms [11].

Table 9. Tools used by detection techniques of DDoS attacks

Techniques	CRF++ toolkits	Globus Toolkit	LIBSVM toolkits	Matlab	Network simulator	SAS Enterpriser Miner	SSFNet simulator	Tstat	Weka	Preset resiliense simulator
[T5]				[32]		[60]			[32]	
[T6]					[68]					
[T7]				[86] [92]				[73]		
[T11]					[26]					
[T12]				[72]	[72]					
[T13]				[70]						
[T14]				[70]						
[T16]				[46]						
[T19]		[73]								
[T21]								[74]		
[T25]										[82]
[T26]				[35] [70]						
[T27]				[63]						
[T29]					[17] [71]					
[T30]					[71]		[16]			
[T33]				[61]		[62]				
[T37]				[63]						
[T38]					[38]					
[T41]	[23]		[23]						[23]	
[T42]				[92]	[96]					
[T43]					[59]					

3.4. Q4: Where are the detection techniques implemented?

DDoS attack detection techniques can be deployed in four locations: source, destination, network and hybrid. Source refers to the source of the attack, while destination is the target of the attack. Network is the place where the information traffic circulates and hybrid means that the detection is performed in multiple places and there is usually cooperation between the points of implementation. Table 10 shows the four sites of implementation together with the authors who use them.

Table 10. Deployment locations where detection mechanisms are implemented

Deployment location	Studies	Total
Source	[37] [50] [56]	3
Destination	[25] [28] [29] [33] [34] [45] [46] [58] [60] [61] [69] [74] [79] [81] [82] [83] [85] [90] [93] [94] [95]	21
Network	[16] [17] [19] [20] [22] [23] [24] [26] [27] [30] [31] [32] [35] [36] [38] [39] [40] [41] [43] [44] [47] [48] [49] [51] [52] [53] [54] [57] [59] [61] [63] [64] [66] [68] [70] [71] [72] [73] [75] [76] [77] [78] [84] [86] [87] [88] [91]	47
Hybrid	[18] [21] [42] [55] [65] [67] [80] [89] [92][96]	10
Total		81

Table 10 shows that Network is where most of the detection techniques have been implemented, that is, approximately 58% of the total amount. This is because the network is the place from which the characteristics of the data flow used by the detection mechanisms can be extracted. Therefore, Network is used by the mechanisms more frequently when implementing a detection technique. On the contrary, the Source is where the techniques are implemented on a smaller scale, because its implementation requires a high degree of cooperation between the data networks, which prevents the construction of a greater number of mechanisms that can predict an attack.

3.5. Q5: At what point in the time should the detection mechanism in an attack be activated?

The detection mechanism can act against a possible DDoS attack Before, During and After [7]. The point in time before refers to prevention of the attack before it happens, while during refers to the moment the attack is being made; and finally, after refers to when the attack occurs at the destination and so can be considered as mitigation. Table 11 shows the points in time in which the detection techniques can act together with the authors that employ them at each location.

Table 11. Point in time when the detection mechanisms are implemented

Point in time	Studies	Total
Before the attack	[21] [37] [42] [50] [56] [89] [96]	7
During the attack	[16] [17] [18] [19] [20] [22] [23] [24] [25] [26] [27] [28] [29] [30] [31] [32] [33] [34] [35] [36] [38] [39] [40] [41] [43] [44] [45] [46] [47] [48] [49] [51] [52] [53] [54] [57] [58] [59] [60] [61] [62] [63] [64] [65] [66] [67] [68] [69] [70] [71] [72] [73] [74] [76] [77] [78] [79] [81] [82] [83] [84] [85] [86] [87] [88] [90] [91] [92] [93] [94] [95]	71
After the attack	[55] [75] [80]	3
Total		81

In Table 11 shows that During is the point in the time where most of the detection techniques have been implemented. This is because the detection in that place is executed in real time, when the attack flow has reached the target. This is because the mechanism analyzes the flow of data while entering the system, when an anomaly is detected this data flow is cut off. On the contrary, After is the moment in which detection techniques are less implemented because the mechanism would have to predict an attack before it affects the system. This process is difficult because continuous communication between the predecessor networks is required to achieve a prediction.

3.6. Q6: What is the precision with which the techniques detect a DDoS attack?

In this research work only studies that had either a detection or an accuracy rate greater than or equal to 98% were considered and where tests with datasets consisting of real flows and DDoS were performed. The detection rate is calculated by means of the following equation: TP detection is equal to $\frac{TP}{TP+FN}$, and accuracy corresponds to $\frac{TP+TN}{TP+TN+FP+FN}$ where, TP = number of true positives, TN = number of true negatives, FP = number of false positives and FN = amount of false negatives. The precision with which the techniques detect a DDoS attack are shown in Table 12.

Table 12. Detection mechanisms of DDoS Attack that showed the best ratios

Detection Rate (%)	Studies	Dataset
99.99	[34]	Knowledge Discovery and Data mining (KDD) Cup 1999
99.67	[86]	CAIDA, TUIDS and DARPA
99.4	[63]	CAIDA 2007, DARPA 2009, BONESI-generated
98.31	[29]	KDD Cup1999

Table 12 shows that the detection mechanism with the highest precision was achieved by [34]. The detection rate of this mechanism was 99.9%. For this, this mechanism uses a combination of three techniques (Random Forest, nearest K-neighbors and Bagging). In addition, the implementation of this mechanism is in the network, so that detection occurs during the attack, so its impact is mitigated when detected by the system. In [86] they proposed a mechanism that uses the correlation technique. The efficiency of this method reaches 99.67%. To do this, it uses the Matlab tool, as well as the implementation of the mechanism is performed on the network during the attack.

It is also observed that the highest efficiency percentages correspond to techniques implemented in the network layer [34], [63], [86]. These techniques employ variables used in the identification of the flow of data such as traffic and TCP flow, as shown in the first mechanism. Whereas in the second mechanism the variables IP address and TCP flow are used, that is, variables used also in the network layer. Therefore, this analysis can establish the need to have alternative mechanisms that evaluate not only the flow of data that circulates through the network, but also measure the user's interaction with the system. In addition, detection mechanisms could be developed that can use other techniques in combination with other variables to achieve greater detection efficiency. In this context, mechanisms could be proposed for detection in other layers where DDoS attacks also occur, such as the application layer. Since, in this layer is where the greatest number of attacks have occurred in recent years due to its easy execution and difficult detection [29].

4. CONCLUSIONS

The systematic review of the literature presented in this study has identified the main aspects involved with the detection of DDoS attacks, focusing on techniques, variables and tools, in addition to the place where it was implemented and the point of detection over time. An analysis of the results has provided answers to the six proposed research questions. In addition, forty eight techniques that are used in the

detection of DDoS attacks were identified. Also, a total of twenty eight variables were observed and it was evident that the most used tools are Matlab and Network simulator, due to the functionalities and advantages of information processing. The most used place for the implementation of a mechanism is the network, because the data flows are analyzed before they reach the server. The most used point in time for the deployment of a technique is during, because the detection is done in real time when the attack occurs. The most effective mechanism to achieve a high detection rate is that proposed by [34], which reached an accuracy of 99.9%, it uses the characteristics of the data flow that is extracted in the network during the attack.

REFERENCES

[1] Tripathi S, Gupta B, Almomani A, Mishra A, Veluru S. Hadoop based defense solution to handle distributed denial of service (ddos) attacks. *Journal of Information Security*, 2013, 4(03), 150.

[2] Waguih H. A data mining approach for the detection of denial of service attack. *IAES International Journal of Artificial Intelligence*, 2013, vol. 2, no 2, p. 99.

[3] Jain A, Singh A. K. Distributed denial of service (ddos) attacks-classification and implications. *Journal of Information and Operations Management*, 2012, vol. 3, no 1, p. 136.

[4] Ni T, Gu X, Wang H. Detecting DDoS Attacks Against DNS Servers Using Time Series Analysis. *Indonesian Journal of Electrical Engineering and Computer Science*, 2014, vol. 12, no 1, p. 753-761.

[5] Criscuolo P J. Distributed denial of service, tribe flood network 2000, and stacheldraht CIAC-2319, *Department of Energy Computer Incident Advisory Capability (CIAC)*. UCRL-ID-136939, Rev. 1., Lawrence Livermore National Laboratory, 2000.

[6] Choi J, Choi C, Ko B, Kim P. A method of DDoS attack detection using HTTP packet pattern and rule engine in cloud computing environment. Soft Computing, 2014, vol. 18, no 9, p. 1697-1703.

[7] Zargar S, Joshi J, Tipper D. A survey of defense mechanisms against distributed denial of service (DDoS) flooding attacks. *IEEE communications surveys & tutorials*, 2013, vol. 15, no 4, p. 2046-2069.

[8] Chen L C, Longstaff T A, Carley K M. Characterization of defense mechanisms against distributed denial of service attacks. *Computers & Security*, 2004, vol. 23, no 8, p. 665-678.

[9] Bhuyan M H, Kashyap H J, Bhattacharyya D K, Kalita J K. Detecting distributed denial of service attacks: methods, tools and future directions. *The Computer Journal*, 2013, 57(4), 537-556.

[10] Wei S, Mirkovic J. Building reputations for internet clients. *Electronic Notes in Theoretical Computer Science*, 2007, vol. 179, p. 17-30.

[11] Oikonomou G, Mirkovic J. Modeling Human Behavior for Defense against Flash-Crowd Attacks. *ICC*. 2009. p. 1-6.

[12] Devi S R, Yogesh P. A hybrid approach to counter application layer DDoS attacks. *International Journal on Cryptography and Information Security (IJCIS)*, 2012, vol. 2, no 2.

[13] Kitchenham B. Procedures for performing systematic reviews. Keele, UK, Keele University, 2004, vol. 33, no 2004, p. 1-26.

[14] Ul Haq M Z, and Suharjito S. Usability Analysis of Business Intelligence Tool Based Table Virtualization. *Indonesian Journal of Electrical Engineering and Computer Science*, 2018, vol. 9, no 2, p. 431-437.

[15] Liu L, Wan P, Wang Y, and Liu S. Clustering and hybrid genetic algorithm based intrusion detection strategy. *Indonesian Journal of Electrical Engineering and Computer Science*, 2014, vol. 12, no 1, p. 762-770.

[16] Beak C, Chaudhry J A, Lee K, Park S, Kim M. A novel packet marketing method in DDoS attack detection. *American Journal of Applied Sciences*, 2007, vol. 4, no 10, p. 741-745.

[17] Meenakshi S, Srivatsa S K. A distributed framework with less false positive ratio against distributed denial of service attack. *Information Technology Journal*, 2007, vol. 6, no 8, p. 1139-1145.

[18] Chen Y, Das S, Dhar P. Detecting and Preventing IP-spoofed Distributed DoS Attacks. *IJ Network Security*, 2008, vol. 7, no 1, p. 69-80.

[19] Yan R, Zheng Q. Using Renyi cross entropy to analyze traffic matrix and detect DDoS attacks. *Information Technology Journal*, 2009, vol. 8, no 8, p. 1180-1188.

[20] Liu H, Sun Y, Kim M S. A Scalable DDoS Detection Framework with Victim Pinpoint Capability. *JCM*, 2011, vol. 6, no 9, p. 660-670.

[21] Tiruchengode N. Dynamic approach to defend against distributed denial of service attacks using an adaptive spin lock rate control mechanism. *Journal of Computer Science*, 2012, vol. 8, no 5, p. 632-636.

[22] Al-Duwairi B, Al-Qudah Z, Govindarasu M. A novel scheme for mitigating botnet-based DDoS attacks. *Journal of Networks*, 2013, vol. 8, no 2, p. 297.

[23] Chen S W, Wu J X, Ye X L, Guo T. Distributed denial of service attacks detection method based on conditional random fields. *Journal of Networks*, 2013, vol. 8, no 4, p. 858.

[24] Udhayan J, Babu M R. Deteriorating distributed denial of service attack by recovering zombies using penalty scheme. *Journal of Computer Science*, 2013, vol. 9, no 11, p. 1618.

[25] Huang C, Wang J, Wu G, Chen J. Mining Web User Behaviors to Detect Application Layer DDoS Attacks. *JSW*, 2014, vol. 9, no 4, p. 985-990.

[26] Sachdeva M, Kumar K. A traffic cluster entropy based approach to distinguish DDoS attacks from flash event using DETER testbed. *ISRN Communications and Networking*, 2014, vol. 2014.

[27] Wang Y, Sun R. An IP-traceback-based packet filtering scheme for eliminating DDoS attacks. *Journal of Networks*, 2014, vol. 9, no 4, p. 874.
[28] Saleh M A, Abdul Manaf A. A novel protective framework for defeating HTTP-based denial of service and distributed denial of service attacks. *The Scientific World Journal*, 2015, vol. 2015.
[29] Johnson Singh K, Thongam K, De T. Entropy-Based Application Layer DDoS Attack Detection Using Artificial Neural Networks. *Entropy*, 2016, vol. 18, no 10, p. 350.
[30] Cepheli Ö, Büyükçorak S, Karabulut Kurt G. Hybrid intrusion detection system for ddos attacks. *Journal of Electrical and Computer Engineering*, 2016, vol. 2016.
[31] Zhou L, Liao M, Yuan C, Zhang H. Low-Rate DDoS Attack Detection Using Expectation of Packet Size. *Security and Communication Networks*, 2017, vol. 2017.
[32] Gu Y, Wang Y, Yang Z, Xiong F, Gao Y. Multiple-Features-Based Semisupervised Clustering DDoS Detection Method. *Mathematical Problems in Engineering*, 2017, vol. 2017.
[33] Mirvaziri H. A new method to reduce the effects of HTTP-Get Flood attack. *Future Computing and Informatics Journal*, 2017, vol. 2, no 2, p. 87-93.
[34] Jia B, Huang X, Liu R, Ma Y. A DDoS attack detection method based on hybrid heterogeneous multiclassifier ensemble learning. *Journal of Electrical and Computer Engineering*, 2017, vol. 2017.
[35] Peraković D, Periša M, Cvitić I, Husnjak S. Model for detection and classification of DDoS traffic based on artificial neural network. *Telfor Journal*, 2017, vol. 9, no 1, p. 26.
[36] Chen S, Song Q. Perimeter-based defense against high bandwidth DDoS attacks. *IEEE Transactions on Parallel & Distributed Systems*, 2005, no 6, p. 526-537.
[37] Mirkovic, J., & Reiher, P. D-WARD: a source-end defense against flooding denial-of-service attacks. *IEEE transactions on Dependable and Secure Computing*, 2005, vol. 2, no 3, p. 216-232.
[38] Yau D K, Lui J, Liang F, Yam Y. Defending against distributed denial-of-service attacks with max-min fair server-centric router throttles. *IEEE/ACM Transactions on Networking (TON)*, 2005, vol. 13, no 1, p. 29-42.
[39] Kim Y, Lau W C, Chuah M C, Chao H J. PacketScore: a statistics-based packet filtering scheme against distributed denial-of-service attacks. *IEEE transactions on dependable and secure computing*, 2006, vol. 3, no 2, p. 141-155.
[40] Yaar A, Perrig A, Song D. StackPi: New packet marking and filtering mechanisms for DDoS and IP spoofing defense. *IEEE Journal on Selected Areas in Communications*, 2006, vol. 24, no 10, p. 1853-1863.
[41] Chen Y, Hwang K, Ku W S. Collaborative detection of DDoS attacks over multiple network domains. *IEEE Transactions on Parallel & Distributed Systems*, 2007, no 12, p. 1649-1662.
[42] Chen R, Park J M, Marchany R. A divide-and-conquer strategy for thwarting distributed denial-of-service attacks. *IEEE Transactions on Parallel and Distributed Systems*, 2007, vol. 18, no 5, p. 577-588.
[43] Wang H, Jin C, Shin K G. Defense against spoofed IP traffic using hop-count filtering. *IEEE/ACM Transactions on Networking (ToN)*, 2007, vol. 15, no 1, p. 40-53.
[44] Chonka A, Singh J, Zhou W. Chaos theory based detection against network mimicking DDoS attacks. *IEEE Communication Letters*, 2009, vol. 13, no 9, p. 717-719.
[45] Ranjan S, Swaminathan R, Uysal M, Nucci A, Knightly E. DDoS-shield: DDoS-resilient scheduling to counter application layer attacks. *IEEE/ACM Transactions on networking*, 2009, vol. 17, no 1, p. 26-39.
[46] Xie Y, Yu S Z. Monitoring the application-layer DDoS attacks for popular websites. *IEEE/ACM Transactions on Networking (TON)*, 2009, vol. 17, no 1, p. 15-25.
[47] Xiang Y, Li K, Zhou W. Low-rate DDoS attacks detection and traceback by using new information metrics. *IEEE transactions on information forensics and security*, 2011, vol. 6, no 2, p. 426-437.
[48] François J, Aib I, Boutaba R. FireCol: a collaborative protection network for the detection of flooding DDoS attacks. *IEEE/ACM Transactions on Networking (TON)*, 2012, vol. 20, no 6, p. 1828-1841.
[49] Yu S, Zhou W, Jia W, Guo S, Xiang Y, Tang F. Discriminating DDoS attacks from flash crowds using flow correlation coefficient. *IEEE Transactions on Parallel and Distributed Systems*, 2012, vol. 23, no 6, p. 1073-1080.
[50] Chen Y, Ma X, Wu X. DDoS detection algorithm based on preprocessing network traffic predicted method and chaos theory. *IEEE Communications Letters*, 2013, vol. 17, no 5, p. 1052-1054.
[51] Luo H, Lin Y, Zhang H, Zukerman M. Preventing DDoS attacks by identifier/locator separation. *IEEE network*, 2013, vol. 27, no 6, p. 60-65.
[52] Wu X, Chen Y. Validation of chaos hypothesis in NADA and improved DDoS detection algorithm. *IEEE Communications Letters*, 2013, vol. 17, no 12, p. 2396-2399.
[53] Luo J, Yang X, Wang J, Xu J, Sun J, Long K. On a Mathematical Model for Low-Rate Shrew DDoS. *IEEE Trans. Information Forensics and Security*, 2014, vol. 9, no 7, p. 1069-1083.
[54] Ma X, Chen Y. DDoS detection method based on chaos analysis of network traffic entropy. *IEEE Communications Letters*, 2014, vol. 18, no 1, p. 114-117.
[55] Wu Y, Zhao Z, Bao F, Deng R H. Software puzzle: A countermeasure to resource-inflated denial-of-service attacks. *IEEE Transactions on Information forensics and security*, 2015, vol. 10, no 1, p. 168-177.
[56] Luo H, Chen Z, Li J, Vasilakos A V. Preventing distributed denial-of-service flooding attacks with dynamic path identifiers. *IEEE Transactions on Information Forensics and Security*, 2017, vol. 12, no 8, p. 1801-1815.
[57] Lee F Y, Shieh S. Defending against spoofed DDoS attacks with path fingerprint. *Computers & Security*, 2005, vol. 24, no 7, p. 571-586.
[58] Al-Duwairi B, Manimaran G. Distributed packet pairing for reflector based DDoS attack mitigation. *Computer*

communications, 2006, vol. 29, no 12, p. 2269-2280.
[59] Chen Y, Hwang K. Collaborative detection and filtering of shrew DDoS attacks using spectral analysis. *Journal of Parallel and Distributed Computing*, 2006, vol. 66, no 9, p. 1137-1151.
[60] Lee K, Kim J, Kwon K H, Han Y, Kim S. DDoS attack detection method using cluster analysis. *Expert systems with applications*, 2008, vol. 34, no 3, p. 1659-1665.
[61] Lu W Z, Gu W X, Yu S Z. One-way queuing delay measurement and its application on detecting DDoS attack. *Journal of Network and Computer Applications*, 2009, vol. 32, no 2, p. 367-376.
[62] Doron E, Wool A. Wda: A web farm distributed denial of service attack attenuator. *Computer Networks*, 2011, vol. 55, no 5, p. 1037-1051.
[63] Kumar P A R, Selvakumar S. Distributed denial of service attack detection using an ensemble of neural classifier. *Computer Communications*, 2011, vol. 34, no 11, p. 1328-1341.
[64] Lee S M, Kim D S, Lee J H, Park J S. Detection of DDoS attacks using optimized traffic matrix. *Computers & Mathematics with Applications*, 2012, vol. 63, no 2, p. 501-510.
[65] Rahmani H, Sahli N, Kamoun F. DDoS flooding attack detection scheme based on F-divergence. *Computer Communications*, 2012, vol. 35, no 11, p. 1380-1391.
[66] Shiaeles S N, Katos V, Karakos A S, Papadopoulos B K. Real time DDoS detection using fuzzy estimators. *Computers & security*, 2012, vol. 31, no 6, p. 782-790.
[67] Wang F, Wang H, Wang X, Su J. A new multistage approach to detect subtle DDoS attacks. *Mathematical and Computer Modelling*, 2012, vol. 55, no 1-2, p. 198-213.
[68] Zhang C, Cai Z, Chen W, Luo X, Yin J. Flow level detection and filtering of low-rate DDoS. *Computer Networks*, 2012, vol. 56, no 15, p. 3417-3431.
[69] Giralte L C, Conde C, De Diego I M, Cabello E. Detecting denial of service by modelling web-server behaviour. *Computers & Electrical Engineering*, 2013, vol. 39, no 7, p. 2252-2262.
[70] Kumar P A R, Selvakumar S. Detection of distributed denial of service attacks using an ensemble of adaptive and hybrid neuro-fuzzy systems. *Computer Communications*, 2013, vol. 36, no 3, p. 303-319.
[71] Seo D, Lee H, Perrig A. APFS: adaptive probabilistic filter scheduling against distributed denial-of-service attacks. *Computers & Security*, 2013, vol. 39, p. 366-385.
[72] Spyridopoulos T, Karanikas G, Tryfonas T, Oikonomou G. A game theoretic defence framework against DoS/DDoS cyber attacks. *Computers & Security*, 2013, vol. 38, p. 39-50.
[73] Varalakshmi P, Selvi S T. Thwarting DDoS attacks in grid using information divergence. *Future Generation Computer Systems*, 2013, vol. 29, no 1, p. 429-441.
[74] Xiao P, Qu W, Qi H, Li Z. Detecting DDoS attacks against data center with correlation analysis. *Computer Communications*, 2015, vol. 67, p. 66-74.
[75] Malialis K, Kudenko D. Distributed response to network intrusions using multiagent reinforcement learning. *Engineering Applications of Artificial Intelligence*, 2015, vol. 41, p. 270-284.
[76] Kalkan K, Alagöz F. A distributed filtering mechanism against DDoS attacks: ScoreForCore. *Computer Networks*, 2016, vol. 108, p. 199-209.
[77] Sachdeva M, Kumar K, Singh G. A comprehensive approach to discriminate DDoS attacks from flash events. *Journal of Information Security and Applications*, 2016, vol. 26, p. 8-22.
[78] Saied A, Overill R E, Radzik T. Detection of known and unknown DDoS attacks using Artificial Neural Networks. *Neurocomputing*, 2016, vol. 172, p. 385-393.
[79] Jazi H H, Gonzalez H, Stakhanova N, Ghorbani A A. Detecting HTTP-based application layer DoS attacks on web servers in the presence of sampling. Computer Networks, 2017, vol. 121, p. 25-36.
[80] MIRVAZIRI H. A new method to reduce the effects of HTTP-Get Flood attack. *Future Computing and Informatics Journal*, 2017, vol. 2, no 2, p. 87-93.
[81] Sreeram I, Vuppala V P K. HTTP flood attack detection in application layer using machine learning metrics and bio inspired bat algorithm. *Applied Computing and Informatics*, 2017.
[82] Nunes I, Schardong F, Schaeffer-Filho A. BDI2DoS: an application using collaborating BDI agents to combat DDoS attacks. *Journal of Network and Computer Applications*, 2017, vol. 84, p. 14-24.
[83] Prasad K M, Reddy A R M, Rao K V. BARTD: Bio-inspired anomaly based real time detection of under rated App-DDoS attack on web. *Journal of King Saud University-Computer and Information Sciences*, 2017.
[84] Behal S, Kumar K. Detection of DDoS attacks and flash events using novel information theory metrics. *Computer Networks*, 2017, vol. 116, p. 96-110.
[85] Singh K J, De T. MLP-GA based algorithm to detect application layer DDoS attack. *Journal of Information Security and Applications*, 2017, vol. 36, p. 145-153.
[86] Hoque N, Kashyap H, Bhattacharyya D K. Real-time DDoS attack detection using FPGA. *Computer Communications*, 2017, vol. 110, p. 48-58.
[87] Li L, Lee G. DDoS attack detection and wavelets. *Telecommunication Systems*, 2005, vol. 28, no 3-4, p. 435-451.
[88] Kulkarni A., Bush, S. Detecting distributed denial-of-service attacks using kolmogorov complexity metrics. *Journal of Network and Systems Management*, 2006, vol. 14, no 1, p. 69-80.
[89] Xiao B, Chen W, He Y. A novel approach to detecting DDoS attacks at an early stage. *The Journal of Supercomputing*, 2006, vol. 36, no 3, p. 235-248.
[90] Kang S H, Park K Y, Yoo S G, Kim J. DDoS avoidance strategy for service availability. *Cluster computing*, 2013, vol. 16, no 2, p. 241-248.
[91] Kang H S, Kim S R. sShield: small DDoS defense system using RIP-based traffic deflection in autonomous

system. *The Journal of Supercomputing*, 2014, vol. 67, no 3, p. 820-836.
[92] Zhou W, Jia W, Wen S, Xiang Y, Zhou W. Detection and defense of application-layer DDoS attacks in backbone web traffic. *Future Generation Computer Systems*, 2014, vol. 38, p. 36-46.
[93] Dick, U., & Scheffer, T. Learning to control a structured-prediction decoder for detection of HTTP-layer DDoS attackers. *Machine Learning*, 2016, vol. 104, no 2-3, p. 385-410.
[94] Prasad K M, Reddy A R M, Rao K V. BIFAD: Bio-inspired anomaly based HTTP-flood attack detection. *Wireless Personal Communications*, 2017, vol. 97, no 1, p. 281-308.
[95] Boro D, Bhattacharyya D K. DyProSD: a dynamic protocol specific defense for high-rate DDoS flooding attacks. *Microsystem Technologies*, 2017, vol. 23, no 3, p. 593-611.
[96] Merouane M. An approach for detecting and preventing DDoS attacks in campus. *Automatic Control and Computer Sciences*, 2017, vol. 51, no 1, p. 13-23.