International Journal of Security and Its Applications
Vol. 12, No. 6 (2018), pp.13-26
http://dx.doi.org/10.14257/ijsia.2018.12.6.02

A Review on Statistical Approaches for Anomaly Detection in DDoS Attacks

Mahsa Nooribakhsh[1], Mahdi Mollamotalebi[2*]
[1, 2] *Department of Computer, Buinzahra branch, Islamic Azad University, Buinzahra, Iran*
[1]*mahsa.nooribakhsh@buiniau.ac.ir*, [2*]*motalebi@qiau.ac.ir*

Abstract

Distributed Denial-of-Service (DDoS) attack is one of the most common and effective type of attacks aiming to deny or weaken the service providing of its victim(s). The disrupting packets of such attack are sent to the victim by several source nodes which made its detection a difficult task. In a distributed attack, several machines cooperate with each other to handle the attack; by this manner, the victim node construed the received traffic behavior as normal. Some aspects such as attacks with low traffic rates, losing the sequential anomaly durations, and the large volume of analysis samples prolong the detection process. The statistical methods, which are reviewed by this article, monitor the receiving traffic in different time periods, and analyze how they are distributed. The memory consumption, computational overhead, attack detection accuracy, detecting the source/destination of the attack, and detection speed are some of the factors affecting the performance of DDoS attack detection systems. The results of this study indicate that among all the above factors, the accuracy and attack detection speed are the most important factors in statistical attack detection systems especially if the detection system acts on the victim's side.

Keywords: *Distributed Denial-of-Service attack, Real-time, Statistical approach, Anomaly detection, Flood attacks*

1. Introduction

The computer network security systems attempt to protect an organization against network attacks. One of the most common attacks in recent years was the DDoS attack. A DDoS attack is designed to inhibit the legal users from accessing their requested services. The attack may occur in the high or low rate of traffic. A high rate traffic attack may be confused with the sudden crowding of packets in the network. On the other hand, the low rate traffic can be construed as normal network traffic. Therefore, detecting such attacks is usually difficult. and detection systems in the literature use Hartley entropy, Shannon entropy, Renyi entropy, Kullback-Leibler divergence, and measurement of the general information gap in order to distinguish between the behavior of normal and attack traffic. In the last decade, scalability of networks and topology changes caused to emerge more DDoS attacks [1]. Mooris, an internet worm, acted as DDoS; it was able to detect and infect vulnerable machines automatically and then replicate itself, saturating the network with a large amount of unwanted messages.

In recent years, DDoS attacks have targeted the accessibility in Internet. One of the most common DDoS attacks is the SYN Bandwidth Flood Attack. Despite to more than twenty years of appearing DDoS attacks, they continue to expand in terms of scope and functionality. In 1999, CIAC released a report on DDoS attacks [2]. In 2000, Amazon,

Received (August 2, 2018), Review Result (October 15, 2018), Accepted (October 21, 2018)
* Corresponding author

ISSN: 1738-9976 IJSIA

Buy.com, CNN and eBay websites were targeted by DDoS attackers by stopping or slowing down the normal service. In 2014, an intense DDoS attack took place on the CloudFlare tool [3], which resulted in an overloading of 400 Gbps and saturation of its network traffic. Also, the 10th annual report on the security of global communications infrastructure [2] claims that Internet bandwidth saturated more than one-third of data centers in 2015 with DDoS attacks. The above and a lot of other evidence indicate the ability of DDoS attacks to affect badly the quality of network services.

The two main models of DDoS attacks include the Agent-Handler model, and the IRC[3]-based model. In the Agent-Handler model, the attacker communicates with the target network for the attack indirectly (through the Handler). Handlers are some infected hosts that control the agents in terms of the type and timing of the attack. Agents are the hosts which are under the attack, although they themselves are not the ultimate target of the attack; they are exploited as an agent to attack the ultimate target. This manner hides the identity of the real attacker and makes the attack detection hard. An IRC channel-based attack operates as multi-user mode so that some common communication channels are used to connect attackers to agents. The users inadvertently act as agents for instant messaging between the attacker and the agents. Allowed IRC ports are used to send the commands to agents. Therefore, it is difficult to follow command packets and causes a lot of traffic on IRC servers so that, the attacker could better hide his presence from the victim's network manager [4]. DDoS attacks can occur in any layer of TCP/IP using different protocols such as ICMP, TCP, HTTP, or UDP.

The methods used to detect DDoS attacks are grouped into two categories: (i) application-based that handles the monitoring and control of packets in the network by the user interface layer; and, (ii) network-based using network protocols in different layers to monitor the network traffic. Also, network-based methods can be based on signature or anomaly detection. A signature-based (or knowledge-based) detection searches previously-identified attack patterns in network traffic packets to detect the security threats (for example, viruses or incomplete packets). Such methods are only capable to detect the known attacks, and the network manager should always add the new attack patterns to the detection system. An anomaly-based detection method, which is focused on current research, detects potential security threats that have abnormal behavior on a set of packets [5].

Given that there are no known models for normal network behavior, it is difficult to provide a definitive system for detecting anomalies. Anomaly detection methods can be categorized as 1) model-based and 2) non-model based methods. In model-based detection, it is assumed that there exists a well-known model for the normal behavior of specific aspects of the network, and any deviation from that behavior is considered as anomaly. But for network behaviors that cannot be described by a model, non-model based approaches are used. Statistical anomaly detection is the most important technique that is based on non-model behaviors. It describes the normal behavior of a particular data as a statistical model and then, performs an inferential statistical test to determine the unknown samples. The statistical techniques do not assume any prior knowledge about the network behavior and are often used to detect flood attacks. Different statistical criteria such as correlation, entropy, covariance, standard deviation, and mutual correlation are used to analyze the network traffic and detect anomaly patterns [6].

The statistical DDoS attack detection techniques provide an appropriate quantitative analysis per packet. But when there are many features to investigate, the computational overhead may increase and if a small set of traffic features are analyzed, correlation statistical methods suffer from low accuracy and high false positive rates. Also, Pearson and Kendall's correlation methods do not work well in real-time conditions with low

[2] https://www.arbornetworks.com/arbor-networks-10th-annual-worldwide-infrastructure-security-report-finds-50x-increase-in-ddos-attack-size-in-past-decade
[3] Internet Really Chat

number of features. Moreover, due to the high rate of traffic in DDoS attacks, software solutions are usually not enough to handle the intensive attack traffic and even, such software systems may themselves be chosen as the target for attack. Due to the low computational complexity of statistical methods in real-time data transfers and their high capability to analyze the network traffic characteristics, the current paper reviews such DDoS detection methods.

This paper is organized as the following. In Section 2, some basic concepts and categorization of anomaly detection methods for DDoS attacks are presented. Then, statistical methods for detection of anomalies are reviewed in Section 3, and section 4 concludes the paper.

2. DDoS attacks and anomaly-based detection methods

In a Denial-of-Service attack (DoS), the attacker makes a host (as victim) very busy by sending frequent requests, and prevents it from the normal activities and addressing the real received requests. This causes reductions in the victim's service performance. The purpose of DoS attacks is to exhaust the resources and disrupt the services that users need to access/use. Today, most of the DoS attacks are applied as distributed (DDoS).

In a DDoS attack, the attacker first scans some remote machines for security holes by some ways/tools such as trojans or worms (for example, by sending email messages containing an infected attachment), and find their vulnerability. Then the attacker infects the above machines (called as zombies or agents) with the attack code. This task is automatically repeated to employ more new zombies. Then, the attacker uses zombies to send attack packets to the target victim. Attackers use spoofing of the source address to prevent or delay attack detection [7].

DDoS attacks have undergone many changes over the past few years with regard to the development of network services/tools for data exchange. In one of the points of view, they are classified based on OSI layer used to attack, the approach for launching the attack, volume of generated traffic, and dynamicity of attack rate. The OSI application, transport, and network layers are typically used for DDoS attacks. In application layer attacks, the protocols such as HTTP and HTTPS are used to flood the traffic into the victim that carries CPU-intensive queries to the target server and makes it too busy. DDoS attacks using network or transport layer (such as TCP SYN flooding, ICMP echo, DNS amplification, and NTP) exhaust the critical resources (e.g. bandwidth, and memory) of the target servers by sending the huge amounts of traffic in layers 3 and 4 to the victim using the protocols such as ICMP, UDP, and TCP.

DDoS attackers may launch sending the attack traffic to victims using the zombies. Another approach (e.g. DNS amplification, NTP, Smurf, and Fraggle attacks) that is named as amplification (or reflection) attack, acts such that an attacker uses several innocent intermediate nodes (reflectors) to handle the attack. The attacker sends requests to the reflectors while spoofing the source IP address by the victim's IP address. Then the reflectors reply to the victims by the messages too larger (amplificated) than the original request size.

In a low-rate DDoS attack such as shrew attack, the traffic rate is not high (but it may be generated by a CPU-intensive query) and is construed as a legitimate traffic. The victim will be exhausted by a high rate of processing instead of a high rate of traffic. On the other hand, high rate DDoS attacks (or flash crowd attacks) send a huge volume of traffic toward the victim. Moreover, based on the dynamicity of attack rate, DDoS attacks are classified into four categories. In constant rate attacks, the attack rate reaches to its maximum degree very soon and creates a sudden packet flood at the victim end. But in increasing rate attacks, the attacker increases the attack rate and observes the victim's reaction in order to evade the victim's detection mechanisms subsequently. Moreover,

some attacks act as pulsing (or periodically) in order to deceive the victim's detection mechanism.

The purpose of a DDoS attack detection system is to detect users/hosts attempting to commit illegal or disturbance acts on the network, and help to how react against the attack. In terms of the position of deployment, detection mechanisms are classified into application-level mechanisms and network-level mechanisms [4]. As mentioned in the previous section, there are two analytical approaches signature-based and anomaly-based to detect malicious activities on the network [2] that, this paper reviews anomaly-based detection methods. Such methods can act as offline exploration or real-time detection. In an offline exploration, the system can detect the attack after it occured (for example, by checking the log files). But a real-time detection system detects the attack at the start point of attack occurrence (in the backbone links of the network).

Different methods have been provided to detect real-time anomaly-based DDoS attacks; however, some difficulties such as attack detection at low traffic rates, the loss of sequential anomalies, and large size of analysis samples causes latency in the detection process. Anomaly-based detection methods for DDoS attacks are classified into five categories as statistical, soft computing, data mining, machine learning, and data stream algorithms . The Statistical methods observe and analyze the input traffic behavior in different time periods. Soft computing-based methods (e.g. neural networks) attempt to classify inbound packets automatically to detect DDoS attacks; such methods suffer from inaccuracy and uncertainty. Data mining and machine learning-based methods use historical network traffic data. They along with classification, association rules, and clustering, extract patterns from network traffic to distinguish between normal and abnormal traffics and subsequently, detect suspicious activities. Data stream algorithms have been provided to analyze large volumes of data as real-time in high-speed networks; they monitor the network traffic stream continuously and make decision instantly.
The techniques based on data mining, machine learning , and soft computing often suffer from high degree of processing that prolongs the detection time; they also suffer from high rates of false positive. On the other hand, the behavior of the data flow may change over time; therefore, it may be necessary to create an online retraining for behavioral characteristics. With regard to rapid increasing of samples and features needed for analysis during the attack occurrence, machine learning algorithms are prone to the bottleneck problem. The statistical methods to detect anomalies are able to do real-time and fast detection of DDoS attacks.

3. Statistical anomaly detection methods in DDoS attacks

To detect the DDoS attacks, various approaches have been presented in recent years. Considering the capabilities of statistical methods for analyzing the behavior of data packets and detecting their anomalies, they are widely used in DDoS attack detection systems. Statistical methods examine user/network behavior priodically in order to detect anomalies. In the following, the statistical methods for anomaly detection in DDoS attacks are reviewed.

Esten et al. [8] provided a data flow sampling method for detecting DDoS attacks in large data flows including two stages of sampling and holding, and then a multi-stage filtering. If there is no flow in the memory (history), a new input is inserted to it for each input packet. When a flow is sampled, a Hash Table[4] counter is stored for it in the flow memory. After recording an input flow, the counter is updated for the subsequent packets and it is not necessary to define a new counter, which reduces the needed memory and potentially it can accelerate packet processing. The filtering used in this method is as multi-stage, in which only packets larger than a threshold value at all stages are sent to the

[4] A data structure to search and store information and has time order of one that is, without considering the number of elements stored, it is only necessary to jump once to find the element.

memory flow. Using sampling, the amount of memory (and process time) needed for each packet is would be reduced. This method is not capable to distinguish between DDoS attacks and flash crowds[5].

The statistical method for the change point detection that has been provided by Wang et al. [9] to detect a SYN flood attack is based on the status of the SYN, FIN[6] and RST[7] flags. In order to determine the detection pattern, a statistical algorithm "non-parametric cumulative sum method" has been proposed that is based on collecting some observations and comparing them with a specific value. The SYN flooding attack is detected through investigating the number of inactive RSTs (by measuring the difference between the total number of SYN and FIN flags). In a normal connection, if the port is closed by sending a packet, RST takes the value 1 which construed as an active RST. The system calculates the attack possibility by measuring the number of inactive RSTs and comparing it with a threshold value; an attack is announced when a sudden change is occurred in the inactive RST's. This method is able to detect the source of an attack, and its computational overhead is low while keeping the detection accuracy high. On the other hand, it works as offline and is not able to detect the attacks as real time. Also, it not able to detect the attacks if there is no a sudden change in the network traffic. Moreover, it does not act efficiently in a network with more than one gateway and it is not suitable for detecting DDoS attacks on large ISPs[8] due to its non-distributed function.

The multi-agent method provided by Peng, et al. [10] uses a sequential non-parametric change point detection to control and monitor increasing of new IP addresses. It detects the attack by observing the sudden changes in the number of packets per source address. This method contains two stages as offline training and detection/learning. In offline training, the learning engine enters the legal IP addresses in a database. The database is updated by arriving new IP addresses, and the expired addresses would be deleted. This action is done as offline to ensure that the information used in the training does not contain any bandwidth attacks. In the detection/learning stage, the statistics of arrived traffic during a time period is collected to extract the proper (normal) time interval. If the arrival rate of new IP addresses is greater than the normal value, a bandwidth attack warning is issued.

This method benefits from the CUSUM algorithm [11] to monitor the random input variables and real-time attack detection. Compared to Wang et al. [9], this method has a higher detection rate and accuracy. However, spoofing the source IP address can deceive this method. In addition, it is able to detect an attack only if a sudden change in the current network traffic occurs.

Chen et al. [12] have presented a centralized method for DDoS attack detection using change points monitoring in a domain (the same method is expanded in [13] as it is able to collaborate between multiple network domains). This method results an on-line alert system to detect DDoS attacks across ISP network domains using the Change Aggregation Tree (CAT). Each domain on the network contains a central CAT server. The routers monitor the network traffic changes, detect suspicious traffic events, and report abnormal traffic patterns to the CAT server. By integrating the CAT subtype tree of different domains, the destination server obtains a general pattern of attack. By gathering warning information from the respective domains, the system can detect DDoS flood attacks. This method acts with high degree of accuracy in detection and provides a distributed solution to detect the attack source. The shortcoming of this method is that it

[5] Flash Crowd: A massive and sudden flow of traffic in a website
[6] It is a flag in the confirmation field. If one of the parties does not have any data for sending, this bit takes the value of 1 in the last packet. Also, the other party must put this bit equal to 1, so that the connection is completely disconnected.
[7] A flag in the confirmation field. If a connection is terminated unilaterally, this bit is equal to 1.
[8] Internet Service Provider

can detect the attack only when a sudden change occurs in network traffic; it is therefore not capable to detect low rate SYN flood attacks.

Chen et al. [14] provided a DDoS attack detection method based on two-sample t-test. The input flow is sampled to obtain the normal SYN arrival rate (SAR). The attack is then detected by calculating the difference between current SAR and normal SAR, as well the difference between number of SYN and ACK packets. This method is capable to detect an attack as real time with high degree of accuracy. Also, its false positive response rate and computational overhead are low. Although it detects DDoS flood attacks if a sudden change in traffic occurs; however, in low traffic conditions, it may be fail to detect an attack.

Udhayan et al. [15] proposed a method called Statistical Segregation Method (SSM) which samples the traffic at sequential time intervals with the aim of distinguish between normal and malicious traffic. By receiving each IP address, SSM considers a counter for it to collect n samples; each sample is a collection of all packets per second. This method compares the obtained samples with the pre-specified conditions of the attack; then it uses correlation analysis to distinguish normal traffic from malicious ones. The time to collect the samples should be deterministic and short. Although collecting more samples can lead to increased accuracy, but it causes more latency in detection and impose additional overheads. Therefore, rapid and effective sampling is required; thus only three samples of each IP address are collected per second, and after an interruption, this action is repeated. Although this method is able to distinguish malicious traffic from a legitimate/normal traffic, when the input traffic rate is high, the detection accuracy is not appropriate.

François, et al. [16] have provided a method called FireCol, with a core consisting of several IPSs[9]. Some rings are arranged virtually around the stations to protect and cooperate with them through the exchange of traffic information vertically. The network traffic information is used in a scoring mechanism to extract the potential attacks. If an attack risk arises, virtual loop communications become horizontal and the risk is measured based on the comparison between the total bandwidth driven to the station with its maximum supported bandwidth.

The FireCol is able to detect some more flooding scenarios such as flash crowd and botnet-based attacks. Each loop consists of some IPSs located at the same distance (same hop count) from the destination station (Client). Each IPS analyzes the traffic information collected during a customizable detection window. Then, the number of iterations and the entropy of each rule are calculated. Each rule describes a specific traffic sample and is in the form of a traffic filter based on the IP address or port number. Having the results of the decision tree, and with adoption of a threshold, both the high and low risk attacks could be detected. This method never deals to false positive problem because it investigates all types of potential attacks with the cost of monitoring all traffic and increasing the detection time.

Ma and Chen [17] have benefited from the entropy chaos analysis and Liaponov's power [18] to detect anomalies in network traffic. The entropy describes the characteristics of the network traffic; however, it depends only on the calculated values of each packet field independently (it ignores the relation between the fields). In DDoS attacks, such as those that spoof the source address, the characteristics are more dispersed and the entropy is capable to detect them. The network traffic is preprocessed by entropy-based methods. Then, DDoS attacks are detected by analyzing the chaos on the entropy of the IP addresses for the source and destination at each time. The results of statistical analysis for this method show that the false positive and false negative values are almost zero, though its processing time is relatively long.

Bhuyan, et al. [19] have evaluated the main criteria for detecting DDoS attacks (such as Hartley entropy, Shannon entropy, and Renyi entropy) in order to early and accurate

[9] Intrusion Prevention System

detect the DDoS attacks. These criteria can be used to describe the network traffic characteristics and to create an effective model for detecting high-rate/low-rate DDoS attacks. To analyze the information criteria, this method monitors the victim's side architecture for real-time network traffic.

The difference (or distance) between legal traffic and attack traffic has been calculated in two high and low traffic rates. Three attributes including the source address, destination address, and protocol, are used for traffic analysis. Except the source address, which is obviously important in detecting service obstruction attacks, this method also uses the destination address to detect the specific traffic flow of a particular destination. Also, the protocol parameter is used to detect and monitor the protocols that attackers use to send harmful traffic. Due to reduced computational complexity, this technique can detect attacks in a shorter time. But in low-level DDoS attacks, there is a short distance between legal and attack traffics which it reduces the accuracy of detection.

Fortunati et al. [20] provided an algorithm to improve the statistical anomaly detection in the network traffic. This algorithm uses covariance criteria to create a profile for common network traffic and detect abnormal activity in the data flow. A revised version of decision-making rules based on the chebyshev difference [21] has been used in order to improve the detection.. In this algorithm, there are decision-making rules that take into account all the information in the covariance matrix. The ROC (receiver operating characteristic curve) has been used to evaluate the performance of this algorithm, especially to reduce the probability of false positive alarms. This algorithm suffers from latency due to considering all information in the covariance matrix and subsequent high computational complexity.

Tao et al. [22] provided a method to detect non-featured DDoS attacks for LANs. The entropy of the packet stream has been applied to network routers. If the network traffic is managed and the entropy of the packet stream drops dramatically over a short period of time, the DDoS attack alert is issued. By using the data gap, DDoS attacks can be distinguished from crowded packet flow. Given that the traffic is triggered by a DDoS attack by a number of agents and they all run the same attack program, the similarity of DDoS attack traffic packets is greater than the similarity of crowded flow issued by different users. This method operates as independent from the attack characteristics (without the need to analyze the previous packets). Its detection is based on the sudden collapse of packet streams' entropy over a short period of time. Therefore, if the attacker sends packets at low rates, this method cannot detect the DDoS attack. Also, if the attack packets are issued by several generator functions, the detection process would be deceived and it is considered as a crowded flow of packets.

Hoque, et al. [23] provided a method based on the analysis of observed traffic behavior which includes two phases. In the first phase, traffic is determined as normal or attack. In the second phase, high and low rate traffics are distinguished. Before these two phases of analysis, a pre-processing step is also done in which, some other features of network traffic (such as the entropy of sources' IP address, the diversity of sources' IP address, and the packet rate) are extracted which are later used in the analysis phase. In this method, a statistical criterion called FFS[10] has been presented for multivariate analysis to differentiate between an attack and normal traffic. In the traffic analysis phase, network packets are sampled in a time window of one second and from each sample, the above three mentioned features are extracted to be used in FFS calculation.

The FFS criterion obtains the similarity degree for an entity using deviation vector and mean of all features' value. If the similarity is less than a threshold value, an attack alert will be issued. The standard deviation vector represents the variation in features' values for the desired entity. The attack traffic includes unpredictable amounts of features, but a

[10] FFS: Feature Feature Score

normal traffic follows a specific pattern. This method acts appropriately in terms of false positive/negative rate in DDoS detection; however, its detection delay is rather high.

Andrysiak et al. [24] provided a method to detect DDoS attacks based on modeling the traffic variability using conditional mean and conditional variance in time series. This method uses the Maximum Likelihood Function to evaluate the traffic characteristics. It benefits from the self-decreasing feature of the ARFIMA [25] and FIGARCH [26] models to summarize the traffic characteristics. To detect unusual behavior which is possibly caused by a network attack, the statistical relationships between predicted traffic and current traffic is used. The results of this method indicate that using ARFIMA model gets a better performance compared to FIGARCH model in terms of the detection rate and false positive.

Özçelik et al. [27] presented a DDoS attack detection approach called CUSUM-Entropy which utilizes the accumulation algorithm (CUSUM) to handle the traffic entropy after a wavelet pre-filtering stage. In this way, this approach do more process on the signal compared to the methods that merely use network traffic's entropy, resulting more efficient attack detection. The entropy measures the data disruption. Increasing the entropy of the source IP address during a DDoS attack reduces the entropy of the destination IP address. This approach is able to use the entropy of other fields in the packet header such as the source port number and protocol type.

The wavelet is used to filter the long-term changes of the observed entropy and reduce the false alarms. The decomposition of a ten-stage wavelet is performed and the components of the tenth low-pass level are filtered. The signal is then reconstructed to filter the entropy data. Finally, the filtered entropy data is processed using the CUSUM algorithm. This method is able to detect DDoS attacks with high precision and low false positive rates; however, normalizing the entropy causes more delay in attack detection.

Hoque et al. [6] provided a real-time detection method for DDoS attacks using a correlation criterion. This method is implemented on FPGA in order to speed up the detection (as it takes less than one microsecond time to categorize traffic as normal or attack). The limitation of most correlation-based statistical methods for DDoS attack detection is that, due to the shift and/or scale correlation between the network traffic characteristics, they are not able to control the false positives; but this method does not have such a weakness. Also, correlation measurements for real-time analysis with a small number of features have low accuracy; but this method has no negative effects on the accuracy. This method calculates the correlation based on the standard deviation of two entities using their mean values. The correlation criterion, unlike the Pearson correlation (that is typical in similar methods), calculates the absolute distance between two entities.

This method analyzes the correlation between the samples with a very small number of parameters (the entropy of the source IP address, the index changes of the source IP address, and the packet rate) which has a significant impact on the real-time DDoS detection; however it cannot distinguish between various DDoS attacks.

Saifullah et al. [28] provided a distributed mechanism to protect the Internet servers against DDoS attacks. It adjusts the loading times of the uploading packets as fairly. In order to control the server traffic, the leaky bucket algorithm is used based on the number of users connected to the routers. Fair division has been achieved by assigning higher bandwidths to the routers connected to more number of users. For a dynamic environment where the number of users changes frequently, a breadth-first search tree is built and each router/server calculates the number of users within its sub-trees. Despite attempting to distribute the work load (that improves the reliability), growing the search tree in this mechanism potentially slows down the process.

Considering the above reviewed the literature, the statistical methods to detect the anomaly-based DDoS attacks and their advantages/disadvantages have been summarized in Table 1.

Ref.	Strengths	Weaknesses	Dataset	Detection Point / Remarks	Features Used in Detection
[8]	Low memory consumption	1. Inability to distinguish between DDoS attacks and flash crowd 2. Delay in detecting attack occurrence	Data generated by NetFlow	The victim's side / Using the multi-stage sampling and filtering to identify the large flows	1. The size of a flow (in bytes) 2. The threshold for large flows 3. The capacity of the link (the number of bytes that can be sent during the entire measurement interval) 4. The number of bytes actually counted for a flow.
[9]	1. Low computational overhead. 2. High detection accuracy. 3. Ability to detect the attack source	1. Ability to detect an attack only if there is a sudden change in the arrived traffic. 2. Lack of distribution. 3. Reliance solely on the volume of traffic sent by the victim	1. Packets transferred by DEC Laboratory 2. Packets transferred by Harvard's campus	The victim's side / Detection of the change point by employing the non-parametric accumulated sum algorithm (CUSUM)	1. TCP SYN, FIN and RST packets
[29]	1. Improved the accuracy and speed. 2. detect attacks with fake IP addresses. 3. Low computational overheads. 4. monitor the IP address of the origin senders.	1. The ability to detect an attack only if there is a sudden change in the behavior of arrival traffic. 2. Lack of distributed capabilities 3. Long detection delays	The network traffic data got from the real network of the research group "Waikato Applied Network Dynamics"	The victim's side / Using a multi-agent method to detect DDoS attacks by monitoring the increases of new IP addresses in packet transfers and issuing the alert if a pre-determined threshold is reached.	1. Fraction of new source IP addresses 2. The mean value of random sequence of IP addresses
[13]	1. Low rate of wrong alerts. 2. Detection of traffic anomalies at very high flow rates	1. Lack of distinguish between flash crowd and DDoS. 2. Able to detect an attack only when a sudden change happened in the arrival traffic behavior	OC48 dataset from the CAIDA project	Network between source and destination / Automatic pursuit of suspicious traffic flows during detecting and modifying the structure of the tree for collecting sudden changes in traffic flow.	1. Deviation from the average number of packets per a time slot 2. Node ID 3. Number of upstream nodes 4. Number of downstream nodes
[14]	1. Low false positive rate. 2. Low computational overhead	1. Weak detection for attacks with low traffic rates. 2. Long detection time	Traffic data generated by the Hoepelnuke V 0.0.2 attack software	The victim's side / Detection of DDoS attack based on two t-test samples by comparing the arrival SYN rate and its normal rate	1. Traffic inertia factor 2. Number of packets received by the routers during a specified time slot
[15]	Reduced false alert rates by distinguishing between legal and malicious traffic with moderate rates	1. Inability of distinguish between attack traffic and legal received traffic in high rate conditions. 2. Long detection times	Data extracted from CAIDA Project	The victim's side / Using the statistical distinguish methods to detect DDoS attacks based on flow sampling at sequential time intervals	1. IP protocol type values 2. Packet size 3. Server port numbers 4. Source/destination IP prefixes 5. Time-to-Live (TTL) values 6. TCP/IP header length 7. TCP flag patterns 8. IP/TCP/UDP checksums
[16]	1. Low false positive rate. 2. High detection accuracy. 3. Appropriate robustness	Potentially increases the detection time due to considering all types of attacks in the overall traffic.	DARPA 99	Network between source and destination / Using virtual loops around the stations to make collaboration between them and adopting a scoring mechanism to guess potential attacks.	1. Frequencies and entropies of the exchanged messages for each customer 2. The maximum bandwidth supported by the customer 3. Traffic filters based on IP addresses and ports
[17]	High detection accuracy	Almost long detection time	LLS DDoS dataset from MIT University	The victim's side / The use of chaos analysis by Liaponov's power to detect anomalies in network traffic	1. Entropies of source and destination IP address 2. Traffic anomalies in a specific time point

[20]	Low rate of false alerts	1. Slowness because of considering the total information of covariance matrix in calculations. 2. Being able to detect an attack only in the case of happening sudden changes in the traffic rate	KDD CUP 99	The victim's side / Using covariance to create profiles of normal traffic and detecting abnormal behavior in data flow; also providing a modified version of decision-making rules based on the chebyshev difference for random vectors	1. Connections to the same host 2. Connections with SYN errors to the same host 3. Connections with REJ errors to the same host 4. Connections to the same service on the same host 5. Connections to different services on the same host 6. Connections to different hosts
[19]	1. Low computational overhead. 2. Short attack detection time	Weak detection accuracy in low traffic conditions	Data from CAIDA project and TUIDS DDoS, and Lincoln Laboratory of MIT	The victim's side / Using the Hartlry, Shannon, and Renyi information metrics, and Kullback-Leibler standard deviation to describe the normal traffic, and detect attacks in real time.	1. Source IP address 2. Destination IP address 3. The used protocol to attack 4. Information distance
[23]	The proper accuracy of distinguishing between normal and abnormal traffic in high and low rate attacks	Almost long detection time	CAIDA DDoS 2007 and MIT DARPA	The victim's side / Extracting the traffic features and providing a statistical metric to analyze their similarity based on the standard deviation and the mean of values	1. Entropy of source IPs 2. Variation of source IPs 3. Packet rate
[24]	Low rate of false positive detection	Summarization have been made for studied features, but anomaly detection does not necessarily mean a DDoS attack.	Using CAIDA [21] and also SNORT IDS [20] as sensors in real networks and collecting statistics of attacks	The victim's side / Use of mean and conditional variances in time series to model and predict network traffic changes, and detecting unusual behaviors. Moreover estimating the accuracy of prediction	1. Number of in/out TCP/UDP packets 2. Number of in/out ICMP packets 3. Number of TCP packets with SYN and ACK flags 4. Number of in/out TCP packets on port 80
[22]	Does not need to analyze previous/historical packets	1. Not able to detect a DDoS attack when low rate of changes occur. 2. If attack packets are issued by several sources, unable to detect an attack.	Attack data generated by Mstream tool	The victim's side / Detection of non-featured DDoS attacks for LANs; applying packet flow entropy on network routers to detect DDoS attacks.	1. Entropy of the flows at a given router 2. Similarities amongst the suspicious flows using abstract information distance metric
[27]	Low rate of false positive detection	1. Long detection time due to more processing on the signal and need for normalization in the entropy. 2. Analysis of only the sources' IP address.	Using the Condor cluster traffic of Clemon University as the source of traffic attack	The victim's side / Applying the total accumulation algorithm (CUSUM) on the observed traffic entropy along with the wavelet filtering.	1. Entropy of source IP address 2. Attack start/stop time 3. Attacker node count information
[6]	1. Low computational overhead 2. High detection throughput 3. No negative effects on accuracy despite using correlation measurement for network analysis.	1. Having limitations on the algorithms able to be implemented on hardware, and difficulty of making changes on it 2. Low sensitivity to attacks compared to the fully-software methods	CAIDA DDoS 2007, MIT DARPA, and TUIDS [24]	The victim's side / Ability of analyzing the correlation between each two samples in traffic with a limited number of characteristics (entropy of the source IP address, index changes of the source IP address, and packet rates); implementation on FPGA to improve the detection speed	1. Entropy of source IP address 2. Variation index of source IPs 3. Packet rate

According to Table 1 and review of the literature, most of the methods used to detect a DDoS attack act as real-time; offline methods usually have high spatial and temporal complexity, and thus, they are not able to detect early attacks. Therefore, they are mostly used to prevent DDoS attacks; however, the results of the offline anomalies exploration can be used to create a reference profile for real-time attack detection. PCA[11] is an

[11] Principal Component Analysis

example of offline statistical methods that monitors the distribution of packet features (such as IP address and ports) in the data flow, and it can detect different types of anomalies. This method, using the entropy as a digest tool (diminishing dimension), is able to categorize the traffic automatically as non-supervised learnt. Although this method detects the attacks rapidly with low rates of false positive, but it suffers from high processing complexity. In another offline method provided by Tan et al. [30], a multivariate correlation analysis (MCA) has been used to extract the geometric correlation between network traffic features. The purpose of this method is to detect known and unknown DoS attacks by learning the legal traffic patterns. Although the attack detection rate of this method is high, it had no evaluation for detection time. It also has not discussed on how it can act as distributed or paralleled to detect an attack [5], and its false positive rate is high.

In recent years, using the combined methods (e.g. statistical methods along with the data mining methods) have been able to tackle the delay of attack detection more appropriately. They also could detect the low rate attacks more accurately. Methods based on the change point detection are highly dependent to occur a sudden different behavior in the received network packets. In contract, methods based on the statistical analyzing of data streams are able to detect the large scale attacks and also distinguish the DDoS attacks from the flash crowd in the network packets. The recent provided methods attempt to speed up the detection in backbone links and reduce the volume of processed data. Moreover, many of early methods provided for DDoS attacks were suffering from the IP spoofing which is eliminated in recent ones (e.g. the methods using the entropy analysis for the traffic packets).

The parameters that are considered in the reviewed methods include the amount of memory consumed, the computational overhead, the accuracy of the attack detection, the ability to identify the attack source/destination, and the delay of attack detection. Also, some attack detection methods are not able to make distinguish between low traffic rate attacks and the normal network flow. Therefore, such weakness is also considered as one of the effective parameters in the reviewed methods. On the other hand, a high volume of traffic flow may be mistaken with a DDoS attack. Therefore, the ability to distinguish between traffic crowd and DDoS attacks is also one of the capabilities that have been addressed in the attack detection systems.

Among the above parameters, the accuracy and delay have a more impressive impact on the quality of detection; the detection point affects on these two important parameters. The detection point may be in the destination network, the victim network, or in the network between the source and destination. Of these, detection on the victim's network is more common; however it potentially increases the use of victim’s network resources. On the other hand, detecting and stopping an attack on the source’s side network is more efficient than the rest though it is challenging operationally (DDoS attacks occur as distributed and the behavior of the source's side hosts may seems quite normal). Detection between source and destination network can be performed with proper accuracy and limited source/destination resource usage; though it requires the collaboration of all median routers which is no guaranteed and thus, it is not possible to assure about practicality of such an approach.

4. Conclusion

The distributed denial-of-service attacks have been developed significantly in recent years with the aim of interrupting a server functions. Therefore, the detection of such attacks and applying some appropriate policies to detect/control them has been studied by many researchers. This paper focused on the methods of detecting statistical anomalies in received packets to reveal the DDoS attacks. Anomaly detection systems first create a

profile for normal behavior of network traffic; and then, any violation or deviation from the normal profile is construed as an abnormal/suspicious behavior.

Today, with increasing data size, DDoS attack detection methods should be able to withstand the high workload of packets exchanged in high-speed network links. Therefore, providing an effective and agile way to detect an attack is essential. Some factors such as memory consumption, computational overhead, attack detection accuracy, ability to identify the source/destination of the attack, and the speed of attack detection, are more attended in attack detection systems. Meanwhile, the detection methods should be able to detect low traffic rate attacks; and conversely, they should not detect mistakenly any high rate traffic as an attack. Misdetection for non-attack packets results in loss of information packets and more overheads.

The results of this research indicate that statistical methods have been recently one of the most efficient approaches of network traffic analysis to detect anomalies in transferred packets. Of all the factors, more important ones in the statistical methods are the accuracy and speed of attack detection. Studies have shown that the improvement of these two factors, with regard to the distribution of DDoS attacks, is highly effective if the attack detection system is deployed on the victim's side network. Due to the growing coverage of cloud computing platforms and the provision of services at various levels to users, DDoS detection systems in cloud computing is recommended as one of the future works. Also, simultaneous use of statistical methods and collective intelligence algorithms potentially help to improve the accuracy of attack detection; however, a probable longer detection time should be considered.

References

[1] Website_Prolexic. (2017). Malicious actors switch tactics to build, deploy and conceal powerful botnets. Available: http://www.prolexic.com/knowledge-center-ddos-attack-report-2014-q2.html
[2] M. H. Bhuyan, H. J. Kashyap, D. K. Bhattacharyya, and J. K. Kalita, "Detecting distributed denial of service attacks: methods, tools and future directions," The Computer Journal, vol. 57, no. 4, pp. 537-556, 2013.
[3] CloudFlare_website. (2017). CloudFlare Available: https://www.cloudflare.com/
[4] T. Peng, C. Leckie, and K. Ramamohanarao, "Survey of network-based defense mechanisms countering the DoS and DDoS problems," ACM Computing Surveys (CSUR), vol. 39, no. 1, p. 3, 2007.
[5] V. Gulisano, M. Callau-Zori, Z. Fu, R. Jiménez-Peris, M. Papatriantafilou, and M. Patiño-Martínez, "STONE: A streaming DDoS defense framework," Expert Systems with Applications, vol. 42, no. 24, pp. 9620-9633, 2015.
[6] N. Hoque, H. Kashyap, and D. Bhattacharyya, "Real-time DDoS attack detection using FPGA," Computer Communications, 2017.
[7] V. L. Thing, M. Sloman, and N. Dulay, "Adaptive response system for distributed denial-of-service attacks," in Integrated Network Management, 2009. IM'09. IFIP/IEEE International Symposium on, 2009, pp. 809-814: IEEE.
[8] C. Estan and G. Varghese, New directions in traffic measurement and accounting (no. 4). ACM, 2002.
[9] H. Wang, D. Zhang, and K. G. Shin, "Detecting SYN flooding attacks," in INFOCOM 2002. Twenty-First Annual Joint Conference of the IEEE Computer and Communications Societies. Proceedings. IEEE, 2002, vol. 3, pp. 1530-1539: IEEE.
[10] T. Peng, C. Leckie, and K. Ramamohanarao, "Detecting distributed denial of service attacks by sharing distributed beliefs," in ACISP, 2003, pp. 214-225: Springer.
[11] E. S. Page, "Continuous inspection schemes," Biometrika, vol. 41, no. 1/2, pp. 100-115, 1954.
[12] Y. Chen and K. Hwang, "Collaborative change detection of DDoS attacks on community and ISP networks," in Collaborative Technologies and Systems, 2006. CTS 2006. International Symposium on, 2006, pp. 401-410: IEEE.
[13] Y. Chen, K. Hwang, and W.-S. Ku, "Collaborative detection of DDoS attacks over multiple network domains," IEEE Transactions on Parallel and Distributed Systems, vol. 18, no. 12, pp. 1649-1662, 2007.
[14] C.-L. Chen, "A New Detection Method for Distributed Denial-of-Service Attack Traffic based on Statistical Test," J. UCS, vol. 15, no. 2, pp. 488-504, 2009.
[15] J. Udhayan and T. Hamsapriya, "Statistical Segregation Method to Minimize the False Detections During DDoS Attacks," IJ Network Security, vol. 13, no. 3, pp. 152-160, 2011.

[16] J. François, I. Aib, and R. Boutaba, "FireCol: a collaborative protection network for the detection of flooding DDoS attacks," IEEE/ACM Transactions on Networking (TON), vol. 20, no. 6, pp. 1828-1841, 2012.
[17] X. Ma and Y. Chen, "DDoS detection method based on chaos analysis of network traffic entropy," IEEE Communications Letters, vol. 18, no. 1, pp. 114-117, 2014.
[18] X. Zeng, R. Eykholt, and R. Pielke, "Estimating the Lyapunov-exponent spectrum from short time series of low precision," Physical Review Letters, vol. 66, no. 25, p. 3229, 1991.
[19] M. H. Bhuyan, D. Bhattacharyya, and J. K. Kalita, "An empirical evaluation of information metrics for low-rate and high-rate DDoS attack detection," Pattern Recognition Letters, vol. 51, pp. 1-7, 2015.
[20] S. Fortunati, F. Gini, M. S. Greco, A. Farina, A. Graziano, and S. Giompapa, "An improvement of the state-of-the-art covariance-based methods for statistical anomaly detection algorithms," Signal, Image and Video Processing, vol. 10, no. 4, pp. 687-694, 2016.
[21] P. L. Butzer and F. Jongmans, "PL Chebyshev (1821–1894) and his contacts with Western European scientists," Historia mathematica, vol. 16, no. 1, pp. 46-68, 1989.
[22] Y. Tao and S. Yu, "DDoS attack detection at local area networks using information theoretical metrics," in Trust, Security and Privacy in Computing and Communications (TrustCom), 2013 12th IEEE International Conference on, 2013, pp. 233-240: IEEE.
[23] N. Hoque, D. K. Bhattacharyya, and J. K. Kalita, "FFSc: a novel measure for low-rate and high-rate DDoS attack detection using multivariate data analysis," Security and Communication Networks, vol. 9, no. 13, pp. 2032-2041, 2016.
[24] T. Andrysiak and Ł. Saganowski, "DDoS Attacks Detection by Means of Statistical Models," in Proceedings of the 9th International Conference on Computer Recognition Systems CORES 2015, 2016, pp. 797-806: Springer.
[25] C. W. Granger and R. Joyeux, "An introduction to long-memory time series models and fractional differencing," Journal of time series analysis, vol. 1, no. 1, pp. 15-29, 1980.
[26] R. T. Baillie, T. Bollerslev, and H. O. Mikkelsen, "Fractionally integrated generalized autoregressive conditional heteroskedasticity," Journal of econometrics, vol. 74, no. 1, pp. 3-30, 1996.
[27] İ. Özçelik and R. R. Brooks, "Cusum-entropy: an efficient method for DDoS attack detection," in Smart Grid Congress and Fair (ICSG), 2016 4th International Istanbul, 2016, pp. 1-5: IEEE.
[28] A. Saifullah, "Defending against distributed denial-of-service attacks with weight-fair router throttling," 2009.
[29] T. Peng, C. Leckie, and K. Ramamohanarao, "Proactively detecting distributed denial of service attacks using source IP address monitoring," in International Conference on Research in Networking, 2004, pp. 771-782: Springer.
[30] Z. Tan, A. Jamdagni, X. He, P. Nanda, and R. P. Liu, "A system for denial-of-service attack detection based on multivariate correlation analysis," IEEE transactions on parallel and distributed systems, vol. 25, no. 2, pp. 447-456, 2014.

Authors

Mahsa Nooribakhsh received the B.Sc. degree in computer engineering from Islamic Azad University of Naragh, Iran, in 2010, and M.Sc. degree in computer engineering from Islamic Azad University of Buinzahra, Iran, in 2015. She is currently a lecturer and researcher in Islamic Azad University of Buinzahra, Iran. Her research interests are network security, cloud computing, recommended systems, project management, and data mining.

Mahdi MollaMotalebi received the B.Sc. degree in computer engineering from Islamic Azad University of Qazvin (QIAU), Iran, in 1999; M.Sc. degree in computer engineering from Islamic Azad University of Arak, Iran, in 2004; and PhD degree in computer science from Universiti Teknologi Malaysia (UTM), Malaysia, in 2013. He is currently a senior lecturer and researcher in Islamic Azad University of Buinzahra, Iran. His research interests are computer network management, computer security, Internet protocols, Grid resource discovery, Cloud computing, Web search engine, and smart home.

