Statistical Properties and Modelling of DDoS Attacks

Pheeha Machaka[1(✉)] and Antoine Bagula[2]

[1] School of Computing, University of South Africa,
Unisa Science Campus, Christiaan de Wet Road & Pioneer Avenue,
Johannesburg 1709, Florida, South Africa
machap@unisa.ac.za
[2] University of the Western Cape, Robert Sobukwe Road, Bellville 7535,
Cape Town, South Africa
abagula@uwc.ac.za

Abstract. The work presented in this paper is an implementation of a design of a DDoS simulation testbed that uses parameter estimation and probability fitting of source IP address features of a network. We explored the issue of lack of adequate and recent evaluation datasets, we therefore designed a way that can be used to generate synthetic data that simulates a DDoS attack. We found that the Gaussian probability distribution best represents the normal operations of a network, while the Poisson probability distribution represents the operations of a network under a DDoS attack.

Keywords: DDoS · EWMA · CUSUM · Attack modelling · Probability fitting

1 Introduction

The rapid transition in information technology has made information more easily available by quicker and cheaper means. The use of these innovations has now changed from the conventional desktop computer to the cellphone and unexpectedly to the Internet of Things (IoT). With this technology, numerous devices that exist in homes, shopping malls, and workspaces will be linked to the internet.

The increased use and reliance of internet technology on society has contributed to a major increase in vulnerabilities. Consequently, large facets of society are directly impacted by any breakdown and damage to the services rendered by these systems. This disturbance can be felt intensely and some can last longer than can be bearable. For example, disruption of an enterprise or government infrastructure can have a major effect on their daily activities [1].

The internet has created a better platform of communication and offered benefits and greater advantages for individuals, organizations and businesses. The proliferated use of the diverse internet devices and products also presents increased security challenges. The internet did not have "security" in its initial design; therefore, attackers have taken advantage of this design glitch. Attackers use easily available malicious tools to carry out attacks on Internet services and products. These attackers have

P. C. Vinh and A. Rakib (Eds.): ICCASA 2020/ICTCC 2020, LNICST 343, pp. 44–54, 2021.
https://doi.org/10.1007/978-3-030-67101-3_4

exploited and taken advantage of devices that are not secured and used these devices as a means to carry out a large scale attack [2].

Recently, Amazon Web Services reported one of the largest DDoS attack in history. In February 2020, they observed and mitigated a 2.3Tbps DDoS attack. In their research they also indicated that there was a 23% increase in DDoS attacks observed in Q1 2020 compared to Q1 2019. Induced disruptions can be caused by efforts of a hacker to harm a system using Denial of Service (DoS) attacks. This is a malicious endeavor by an attacker to interrupt a service provider in order to render it inaccessible to customers. The large-scale variation is the Distributed Denial of Service (DDoS). Such intrusions could have catastrophic consequences on an organisation. This can contribute to dissatisfied clients and substantial damages; this can also see forfeiture of intellectual property, which then affects the longevity of corporations and governments in economic and commercial sustainability. Therefore, it is necessary for organizations and governments to adopt strategies that will help them effectively identify the start and frequency of DDoS attacks [3].

There are two types of NIDS, firstly, signature-based detection systems seek to describe a collection of templates that determine if a specified network traffic sequence is an intrusion. If the traffic pattern fits the classification in the database, then it can be accurately detected. Consequently, in detecting intrusions, signature-based systems achieve high levels of accuracy and low false positive rate. However, they are not able to accurately identify new attacks or modifications of known attacks. Therefore, the impetus for the development of anomaly-based NIDS was the shortcomings of signature-based intrusion detection. The second anomaly based intrusion detection systems (ABIDS) identify events based on a 'natural' system's activity that tend to be anomalous. An intrusion is reported when an abnormality from standard network activity has been detected. There are some inherent drawbacks to anomaly-based detection. First, advanced attackers could observe the network traffic in order to train the attacking systems. Second, the intricacy of establishing the optimum threshold contributes to a rise in the false positive rate. Finally, I can be challenging to abstract valid and anomalous network activity characteristics both qualitatively and accurately [4].

A significant number of DDoS attacks assume the format of a constant attack rate. The attack agent generates attack packets that are dispatched at a consistent and continuous pace from the outset of this form of attack. Attack agents create packets without breaking or changing the attack rate. The effect on a victim of such an attack is rapid, persistent and sudden. Signature-based identification strategies make it simple to identify these forms of attacks.

In order to avoid detection, attackers have adapted their attack tactics and have planned low-rate attacks strategy. This strategy will steadily increase to deplete all machine resources. By steadily weakening the services of the victim over an extended period, this technique obstructs the identification of the attack. Depending on the response of the victim to the attack, these kinds of attacks will change their attack rate. In this type of assault, the victim will encounter a periodic interruption of operation since the attack will often alleviate the victim's attack impact in order to avoid detection.

While a large number of systems were developed in the past to address this problem, there are still challenges in research. Some of them being the issue of (1) dimensionality in traffic features; and (2) choosing a better statistical probability

distribution that is best fits for modelling traffic data using of synthetic dataset due to the lack of good quality datasets.

Therefore, this paper attempts to answer the following research question: (1) Researchers have used features of incoming packets source IP address as a helpful metric to identify the start of an attack. However, high dimensionality in IP address features and the complicated correlation between them causes heavy computational overheads and make the detection task challenging. We therefore question how the onset of the DDoS attack can be identified on the basis of simple features of the source IP address? (2) Current DDoS attacks datasets have constraints: these are privacy and legal concerns involved with the sharing of recorded datasets. Thus, there is a lack of actual intrusion data that could be used to simulate attacks and to test and validate new detection techniques. From this challenge, we therefore ask: What are the key statistical features of a DDoS attack? How do we model the characteristics of DDoS attacks so that we can simulate and produce practical attack traffic datasets?

2 DDoS Attacks Detection

Kaspersky Lab's 2020 s quarter report showed that the most common attack technique was the TCP SYN flooding attack. The TCP SYN flood accounted for 94.7%, while the ICMP attacks accounted for 4.9%, and other types of DDoS attacks were sidelined [5]. It is for this reason that the TCP SYN attack is the main subject of investigation this paper. The attack methods of the TCP SYN DDoS attack are further elaborated below. This is followed by a background research on detection techniques that use the IP address, and their challenges are also explored.

2.1 TCP SYN Flooding Attack

This is the most common and effective network layer flooding attack. The susceptibilities of the normal TCP three-way handshake are exploited; as shown in the figure below. The client will initiate the connection on a standard TCP connection by sending a SYN packet to the server requesting a connection. The server will open a session after receiving the request and replies with a SYN-ACK; it records the information of the initiated TCP connection in the database while it allocates resources to that session [6].

The session will carry-on in a half-open state, the SYN RECVD state. To finalise the connection with the server, the client will need to approve the connection and reply to it with an ACK packet. The server then scans the memory for a current request for a connection and transfers the TCP connection from the SYN RECVD state to the ESTABLISHED state. If no ACK packet is sent within a given time, the link will be delayed and the allocated resources will not be released [7].

The intruder floods the victim server with SYN packets in this attack. These packets usually contain IP addresses that are spoofed, these are addresses do not exist or unused. It is also possible to initiate TCP SYN floods using corrupted agents with valid IP addresses, but the agents need to be positioned so that the victim server does not respond or recognize it. In this way, the server for the partially open connection request will not be in receipt any acknowledgement packets from the clients (Fig. 1).

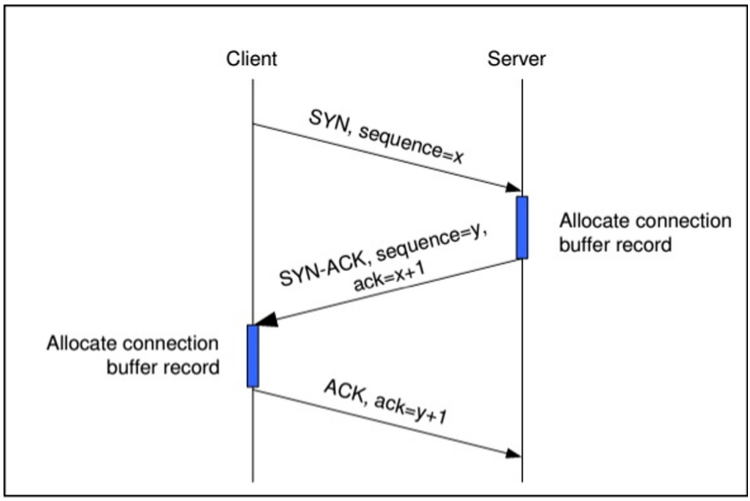

Fig. 1. TCP Three-way Handshake

The server maintains a significant amount of incomplete three-way handshake during the high-rate flooding attack and allocates resources to fake connection requests for a period of time. More fake requests will be collected by the server and its resources will inevitably be depleted. This will prevent further processing of new requests, plus legitimate client requests, by the server [8]. The section that follows explores the use of the IP address for detecting DDoS attacks and the benefits and challenges faced with using IP address as a detection feature.

2.2 DDoS Attack Detection Using IP Address

For information exploration in machine learning, feature selection is important. In the selection of features, researchers pick a subset of relevant data features to develop robust and powerful machine learning models for the detection of intrusions. By finding significant data characteristics and how they correlate, this allows to create a deeper understanding of the data. This will boost the learning model 's efficiency in many ways and help reduce the effect of the issue of high dimensionality. New DDoS attacks have come to light with the emergence of big data and the consequent criteria for successful machine learning techniques, and creative detection approaches are in demand [9].

The importance of feature selection cannot be underemphasized. It is central to any detection method and algorithm because it helps identify those features that are intrinsic of a network attack traffic, and normal network traffic. However, the main challenge that researchers face in designing an effective detection technique is the issue of high dimensionality in network traffic data and the high computational costs it incurs. High dimensionality in network traffic data and the complicated correlation between the features causes heavy computational overheads and make the design of an anomaly detection particularly challenging.

The major challenge with using IP address for a detection technique is the issue of scalability. For an IPv4, the researcher need to compute and store statistical information for 232 elements of the IP address space. This requires large computational and storage overheads, and requires monitoring fewer IP addresses during normal traffic and during an attack. The design of detection technique become even more challenging when it relates to an IPv6 address space were the quantity of elements in the address space increases to 2128 [10].

Over time, researchers have used different features related to IP addresses to design detection techniques for DDoS attacks. Efforts have been made to use IP address characteristics such as IP address traffic volume, adjust the number of different network flows, i.e. a grouping of destination and source IP, destination and source port, and the protocol type [11]. The work of researchers in [12] focus their detection efforts on using incoming traffic volumes and IP address distribution. The researchers also used entropy to further measure IP address distribution and uniformity. They group traffic flows according to the destination IP addresses and they compare each group's traffic volumes to the predicted chi-square statistic. A divergence from the expected traffic profile will signify an attack. The work of researchers in [13, 14] also evaluated entropy measures across IP header features. These use of entropy is a measure of features distribution to detect when there is a deviation in the network traffic performance.

Some researchers have used historical database mechanisms to maintain a list of valid IP addresses. These are IP addresses for whom a three-way TCP handshake has been completed. In order to maintain a recent IP addresses database, this technique uses a sliding window update. During an attack or when the network is overloaded, only those packets from IP addresses listed in the database are accepted [15]. This technique can be outwitted by a crafty attacker by establishing a TCP handshake for the purpose of launching an attack later with various IP addresses.

Some researchers have tried to differentiate flash events from DDoS attacks using the IP address. Flash events (FE) occur when a network server encounters a sudden growth in traffic requests from genuine and authentic clients, however, this sudden increase can be likened to a high rate DDoS attack. In order to differentiate FE's and to also detect DDoS attacks, researchers in [16] used an IP address aggregation technique. The technique makes the assumption that during an FE, most clients' IP addresses will be geographically nearby, while for a DDoS attack, IP addresses will be widely distributed. The section that follows will explore the use of IP address and probability distribution fitting for the purpose of modelling a DDoS attack.

3 DDoS Attack Modelling

In this research, we aim to present methods that can be used for modelling DDoS attacks for the purpose of designing detection techniques against these attacks. We first explore the type of datasets that are used by researchers, the benefits and challenges that researchers face using these datasets. We also explore the probability distributions that are used for differentiating and fitting normal network traffic and network traffic under a DDoS attack. We further explore how researchers can generate synthetic data using that emulates a DDoS attack.

3.1 Datasets Used for Modelling

The research area of network anomaly detection continues to develop, and with good datasets, it is important to evaluate developed detection methods. There are several network intrusion datasets that were created by prominent research groups. The efforts were to assist with the assessing and validating developed techniques and algorithms. A superior dataset assists researchers to identify the efficacy of developed methods to detect attacks when implemented in actual operating environments.

Researchers have used several public dataset, private datasets and network simulated datasets. However most researcher have referenced the publicly available datasets like the DARPA Dataset, KDD Cup dataset, NSL-KDD Cup dataset, DEFCON dataset and the CAIDA dataset. These are yardstick datasets produced using experimental environments [9]. For this research the DARPA dataset was used for its popularity of use in the field of DDoS attack detection. However, this dataset has its own challenges.

For researchers, the natural problem with evaluating the designed techniques for detecting DDoS attacks is the insufficiency of openly obtainable real-word network traffic datasets. The datasets that normally earn reference are usually out of date for correctly demonstrating the latest traffic directions. Due to the legal and privacy issues, they have been removed off sensitive data. Therefore, the majority of research on this topic are evaluated using open-source traffic generators, testbeds based on simulations and publicly available datasets. Each of these evaluation strategies have their own limitations. Therefore, these limitations have lead researchers to developing testbeds that are low cost, customizable and scalable [17].

3.2 Probability Distribution Functions for DDoS Attack Detection (Modelling)

In anomaly-based detection systems, researchers design detection systems by modelling the normal behavior of an attack free network traffic. In the event that a abnormality from the standard behavior is detected, then an attack would be detected. A DDoS attack brings about unexpected changes in the network traffic. Likewise, an unexpected variation in the statistical features of network traffic performance can be noticed. Should there be a DDoS occurrence at a particular time λ, the data will depict a substantial statistical variation about or from the time larger than λ [18].

The literature [19] has shown that statistical and mathematical behavior of these attacks is usually regarded as entropy and the information theory of network traffic characteristics. These metrics capture the unusual distributional changes of the traffic data features in a single value. Therefore, sufficient observations of the changes in the value can distinctly reveal the anomalies in the network therefore distinguishing attack traffic from normal traffic. Researchers have studied various probability distributions to capture the intricacy of the statistical properties of a DDoS attacks. The Weibull, Gaussian and Logistic distributions are the most popular. The Weibull probability distribution function is generally used to represent and to model traffic features. To represent network traffic data, the Gaussian probability distribution model is often commonly used, while logistic regression distribution models are often used in the field of network traffic and attack modeling [20].

It is important for researchers to further understand which distribution model is best suitable for DDoS attack detection. This will assist with building and designing more accurate detection techniques and algorithms. The work of researchers in [20] looked at implementing probability fitting and parameter estimation on many features of a DDoS attack. They provided probabilistic behavior of traffic features of DDoS attacks. They found that the best fitted probability distribution for TCP SYN DDoS attacks is the Weibull, Gaussian and Logistic distribution. This is further confirmed by the work of researchers in [21]. Based on their analysis, they found that under normal legitimate network traffic, where humans were participating, and the probabilistic characteristics of the network data was that of a Gaussian distribution. In the instance were a DDoS attack is launched, where the network traffic data is auto-generated by bots or agents, the probabilistic character of the network data resembled that of a Poisson distribution. For the design of the DDoS attack testbed, we used the Poisson distribution for generating synthetic attack data.

3.3 Synthetic Network Traffic Modelling

Researchers are faced with the challenge of obtaining realistic datasets, and the datasets that are currently available are too old and do not reflect the latest trends. To overcome this challenge many researchers have developed a customized traffic generation testbed simulation in order to evaluate designed techniques. It is for this reason that we used a similar approach in this research.

For the purpose of modelling attack traffic data, in this research we analyzed the attack-free data from various source IP addresses in the DARPA dataset. This is a dataset from the MIT Lincoln Laboratory that was compiled using real traffic data. The data includes trace data from network traffic collected in normal network operation. We examined traffic data in this experiment where there were noteworthy traffic operations. Thus, from 08h00–19h00, so 11 h of traffic data was considered. The dataset was filtered by the source IP address and TCP protocol and the TCP SYN was collected. When investigating the onset of a TCP SYN flood attack, we considered SYN packets.

The examination considered the calculation of SYN packets at intervals of 10 s. This was done so that these attacks were synthetically created to enable investigations of the performance of an algorithm across various attack characteristic scenarios. They were produced using a homogenous Poisson process that generates independent and exponentially distributed delays between packet arrivals. The attack was designed to extend over 30 time intervals (each time interval is 10-s) for 300 s (five minutes). Every five-minute traffic period was injected with attack data to contemplate all potential attacks used for these experiments. We consider and model two kinds of attack characteristics in these experiments: high and low intensity attacks. The particulars of these traffic features will be explained next.

Those attacks whose intensity gradually increases until all resources are depleted are low intensity (or low rate) attacks. By steadily weakening the services of the victim over a prolonged period of time, this technique delays the identification of the attack. For the experiments, we found that a low-intensity attack has its mean amplitude at 50 percent higher than the mean of the normal traffic in a five minute attack interval. Figure 2 reflects this. Between intervals of 20–40, attacks were synthetically injected.

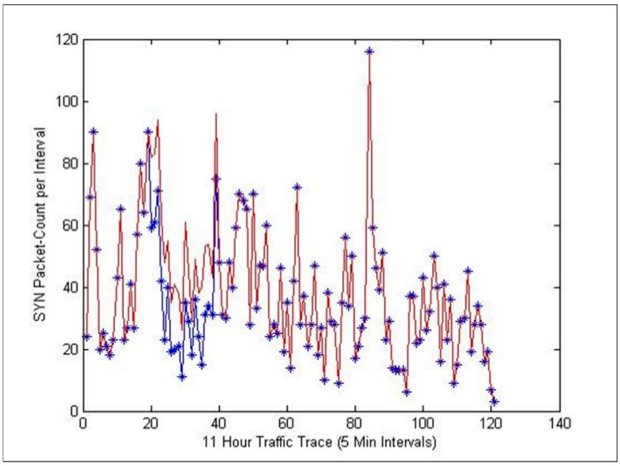

Fig. 2. Low intensity attacks (red line) seen on interval 20–40. (Color figure online)

High rate attacks were found to have an abrupt increase and reach the highest amplitude in a single attack interval. During the attack, packets are directed at a stable and continuous rate, without a halt or deviation in the attack rate. The victim impact is rapid and abrupt [22]. In our experiments, high rate attacks 250% above the mean packet rate in that given interval. This can be noticed between the same interval 20 and interval 40 of Fig. 3.

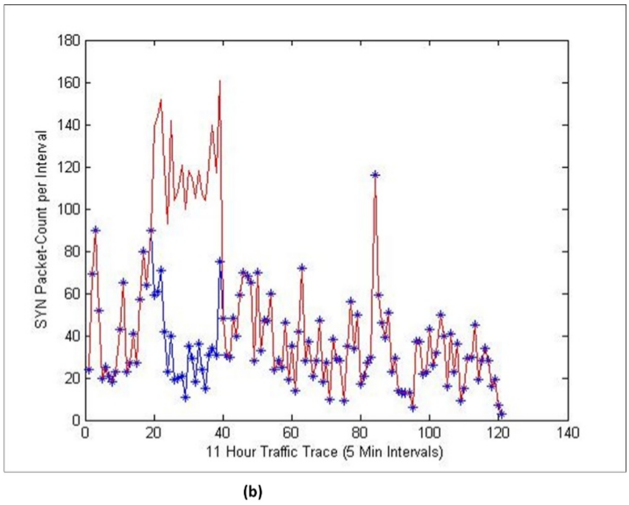

Fig. 3. High Intensity attacks (red line) seen on intervals 20–40. (Color figure online)

In these experiments, we used the Poisson distribution flow to simulate a DDoS attack traffic, and we assumed a Gaussian distribution for normal network traffic. The Poisson distribution flow used the function: $f_P(k;\lambda)$ were the non-negative integer $k \in [0;\infty]$ and the positive real number λ is the average packet rate per second for a given time interval.

4 Implementation Results and Discussions

The implementation and development of this testbed was in MATLAB. To test the efficacy of the testbed, two change point detection algorithms were deployed. We use the Cumulative Sum (CUSUM) and the Exponentially Weighted Moving Averages (EWMA) algorithms. The implementation details of these algorithms are further elaborated below.

The CUSUM and EWMA belong to a family of change point detection techniques [23, 24]. These algorithms based on the assumption of statistical testing and were developed for independent and identically distributed random variables $\{y_i\}$. In the approach, a sudden change arising at a given time can be modeled using two hypothesis, θ_0 and θ_1. θ_0 represents the statistical properties before the sudden deviation; θ_1 represents the statistical properties after the sudden deviation. The hypothesis testing in our experiments depend on the condition of the network, attack or normal condition. Thus, this is defines as follows:

- θ_0: There is no DDoS attack and has the probability distribution f_0,
- θ_1: There is a DDoS attack and has the probability distribution f_1.

These simulations examined the functioning of the CUSUM and the EWMA algorithms performance against DDoS attacks both low and high rate attacks. We also investigated the balance amongst the algorithms' detection rate, false alarm rate and detection delay.

For the EWMA simulation experiments, and for high intensity DDoS. The algorithm was able to detect high intensity DDoS attack with a detection accuracy of 100%, although the false positive rate continued at an average of 30%. The experiments further revealed that the detection delay was on average between 11–23 s. Thus the algorithm was able to detect, with accuracy, high rate attacks 11–23 s after its onset. For low rate attacks, the EWMA algorithm detects attack with 100% accuracy, however, the false positive rate increased to between to 40%–60%. The EWMA algorithm was able to accurately detect a low intensity attack, on average, 40 s from its onset. More details and results can be found in this publication paper [25].

For the CUSUM algorithm simulation experiments, and for high rate DDoS attacks, the algorithm detects DDoS attacks with a detection rate of 100% whereas having a false positive rate that is between 0% and 7%. The CUSUM algorithm had accurately detected high rate DDoS attacks on average between 26 s to 45 s from its onset. For the case of low rate DDoS attacks, the CUSUM algorithm yielded 14%–81% detection rate but maintaining a low false positive rate that is from 0% to 7%. Even though the CUSUM algorithm could not reach a full detection accuracy, the fastest detection delay

was recorded as 73 s detection delay from the onset of an attack. More details and results of this simulation can be found in this publication [26].

The results of the simulation testbed has shown that the algorithms were able to accurately detect high intensity attacks with a fairly reasonable false positive rate and detection delays. However, these algorithms have drawbacks when a low intensity DDoS attack presents itself in network. This further indicates that there is room for improvement in terms of accurately detecting the cunning techniques of a low intensity DDoS attack.

5 Conclusion and Future Work

The work presented in this paper is an implementation of a design of a DDoS simulation testbed that uses parameter estimation and probability fitting of source IP address features of a network. We explored the issue of lack of adequate and recent evaluation datasets, we therefore designed a way that can be used to generate synthetic data that simulates a DDoS attack. We found that the Gaussian probability distribution best represents the normal operations of a network, while the Poisson probability distribution represents the operations of a network under a DDoS attack.

Researchers have often used source IP address in combination with other network traffic features to design DDoS attack detection algorithms. However, this has often lead to the issue of high dimensionality in data. In these experiments we used the source IP address only to find out if a single network traffic feature can be used for the detection of DDoS attacks. We used various scenarios of network attacks were we considered high intensity attacks and low intensity attacks.

To further evaluate the testbed, we deployed two change-point detection algorithms, namely the EWMA and the CUSUM algorithms. The deployment yielded positive results and also indicated areas of improvement. We plan to further intend to implement a deep learning algorithm on this testbed to further evaluate it with more complex and recent detection algorithm so that we can learn more about the efficacy of the testbed for future use.

References

1. Gluhak, A., et al.: A survey on facilities for experimental internet of things research. Commun. Mag. IEEE **49**(11), 58–67 (2011)
2. Mirkovic, J., Reiher, P.: A taxonomy of DDoS attack and DDoS defense mechanisms. ACM SIGCOMM Comput. Commun. Rev. **34**(2), 39–53 (2004)
3. Forrester Consulting. “The trends and Changing Landscape of DDoS Threats and Protection” (2009)
4. Bhattacharyya, D.K., Kalita, J.K.: DDoS Attacks: Evolution, Detection, Prevention, Reaction, and Tolerance (2016)
5. Kupreev, O., Badovskaya, E., Gutnikov, A.: Kaspersky Report: DDoS attacks in Q2 2020 (2020)
6. Douligeris, C., Mitrokotsa, A.: DDoS attacks and defense mechanisms: classification and state-of-the-art. Comput. Netw. **44**(5), 643–666 (2004)

7. Bhuyan, M.H., et al.: Detecting distributed denial of service attacks: methods, tools and future directions. Comput. J. **57**, bxt031 (2013)
8. Mirkovic, J., Reiher, P.: D-WARD: a source-end defense against flooding denial-of-service attacks. IEEE Trans. Dependable Secure Comput. **2**(3), 216–232 (2005)
9. Bhuyan, M.H., Bhattacharyya, D.K., Kalita, J.K.: Network traffic anomaly detection techniques and systems. In: Network Traffic Anomaly Detection and Prevention (2017)
10. Ahmed, E., et al.: Use of ip addresses for high rate flooding attack detection. In: IFIP International Information Security Conference (2010)
11. Barford, P., Plonka, D.: Characteristics of network traffic flow anomalies. In: Proceedings of the 1st ACM SIGCOMM Workshop on Internet Measurement (2001)
12. Feinstein, L. et al.: Statistical approaches to DDoS attack detection and response. In: Proceedings DARPA Information Survivability Conference and Exposition (2003)
13. Lakhina, A., Crovella, M., Diot, C.: Mining anomalies using traffic feature distributions. ACM SIGCOMM Comput. Commun. Rev. **35**(4), 217–228 (2005)
14. Wagner, A., Plattner, B.: Entropy based worm and anomaly detection in fast IP networks. In: 14th IEEE International Workshops on Enabling Technologies: Infrastructure for Collaborative Enterprise (WETICE'05) (2005)
15. Peng, T., Leckie, C., Ramamohanarao, K.: Protection from distributed denial of service attacks using history-based IP filtering. In: IEEE International Conference On Communications, ICC 2003 (2003)
16. Le, Q., Zhanikeev, M., Tanaka, Y.: Methods of distinguishing flash crowds from spoofed DoS attacks. In: 2007 Next Generation Internet Networks (2007)
17. Bhatia, S., et al.: A framework for generating realistic traffic for distributed denial-of-service attacks and flash events. Comput. Secur. **40**, 95–107 (2014)
18. Tartakovsky, A.G., Polunchenko, A.S., Sokolov, G.: Efficient computer network anomaly detection by changepoint detection methods. IEEE J. Select. Topics Signal Process. **7**(1), 4–11 (2013)
19. Bhuyan, M.H., Bhattacharyya, D., Kalita, J.K.: An empirical evaluation of information metrics for low-rate and high-rate DDoS attack detection. Pattern Recog. Lett. **51**, 1–7 (2015)
20. Erhan, D., Anarım, E.: Statistical properties of DDoS attacks. In: 2019 6th International Conference on Control, Decision and Information Technologies (CoDIT) (2019)
21. Li, K. et al.: Effective DDoS attacks detection using generalized entropy metric. In: International Conference on Algorithms and Architectures for Parallel Processing (2009)
22. Machaka, P., Nelwamondo, F.: Data mining techniques for distributed denial of service attacks detection in the internet of things: a research survey. In: Data Mining Trends and Applications in Criminal Science and Investigations (2016)
23. Page, E.: Continuous inspection schemes. In: Biometrika, pp. 100–115 (1954)
24. Roberts, S.: Control chart tests based on geometric moving averages. Technometrics **1**(3), 239–250 (1959)
25. Machaka, P., Bagula, A., Nelwamondo, F.: Using exponentially weighted moving average algorithm to defend against DDoS attacks. In: 2016 Pattern Recognition Association of South Africa and Robotics and Mechatronics International Conference (PRASA-RobMech) (2016)
26. Machaka, P., et al.: Using the cumulative sum algorithm against distributed denial of service attacks in internet of things. In: International Conference on Context-Aware Systems and Applications (2015)