proceedings

MDPI

Proceedings

A Machine Learning Approach for DDoS (Distributed Denial of Service) Attack Detection Using Multiple Linear Regression †

Swathi Sambangi * and Lakshmeeswari Gondi *

Department of Computer Science and Engineering, GITAM University, Visakhapatnam, Andra Pradesh 530045, India

* Correspondence: ssambangi555@gmail.com (S.S.); gondi.lakshmeeswari@gmail.com (L.G.)

† Presented at the 14th International Conference on Interdisciplinarity in Engineering—INTER-ENG 2020, Târgu Mureș, Romania, 8–9 October 2020.

Published: 25 December 2020

Abstract: The problem of identifying Distributed Denial of Service (DDos) attacks is fundamentally a classification problem in machine learning. In relevance to Cloud Computing, the task of identification of DDoS attacks is a significantly challenging problem because of computational complexity that has to be addressed. Fundamentally, a Denial of Service (DoS) attack is an intentional attack attempted by attackers from single source which has an implicit intention of making an application unavailable to the target stakeholder. For this to be achieved, attackers usually stagger the network bandwidth, halting system resources, thus causing denial of access for legitimate users. Contrary to DoS attacks, in DDoS attacks, the attacker makes use of multiple sources to initiate an attack. DDoS attacks are most common at network, transportation, presentation and application layers of a seven-layer OSI model. In this paper, the research objective is to study the problem of DDoS attack detection in a Cloud environment by considering the most popular CICIDS 2017 benchmark dataset and applying multiple regression analysis for building a machine learning model to predict DDoS and Bot attacks through considering a Friday afternoon traffic logfile.

Keywords: DDoS attack; multiple linear regression; traffic packet; classification; Cloud

1. Introduction

Historically, Denial of Service (DoS)attacks are intended primarily to disrupt computing systems in a network. Fundamentally, these attacks are initiated from a single machine with the illegitimate intension of targeting a server system through an attack. A simple DoS attack could be a PING Flood attack in which the machine sends ICMP requests to the target server and a more complex DoS attack example could be Ping of death attack. DDoS (Distributed Denial of Service) attacks are postcursor to DoS attacks, i.e., DoS attacks are forerunner to DDoS attacks. DDoS attacks are the attacks which are carried in distributed environments. Fundamentally, a DDoS attack is an intentional attack type which is usually made in a distributed computing environment by targeting a website or a server so as to minimize their normal performance. To achieve this, an attacker uses multiple systems in a network. Now, using these systems, the attacker makes an attack on the target website or server by making multiple requests to the target system or server. As these types of attacks are carried out in distributed environments, hence, these are also called distributed DDoS attacks.

The conventional way of DDoS attacks is the brute force attack that is triggered using Botnet wherein the devices of the network environment are infected with malware. Based on the target and the behavior, we may classify DDoS attacks into three categories. Thus, though DDoS attacks could be

categorized into several types, usually these attacks are mainly classified into three classes. They are (i) Traffic/fragmentation attack, (ii) Bandwidth/Volume attack and (iii) Application attack as shown in Figure 1. In traffic-based attacks, voluminous UDP or TCP packets are sent to the target system by the attacker and these huge UDP or TCP packets reduce the system performance. In the second type of attack called bandwidth or volumetric attacks, the attacker creates congestion in bandwidth through consuming excessive bandwidth than required legitimately and they also try to flood the target system through sending large amounts of anonymous data. The last type of attack are also specialized attacks as they are aimed at attacking only a specific system or a network. These types of attacks are also difficult to mitigate and throw greater challenges in recognizing them.

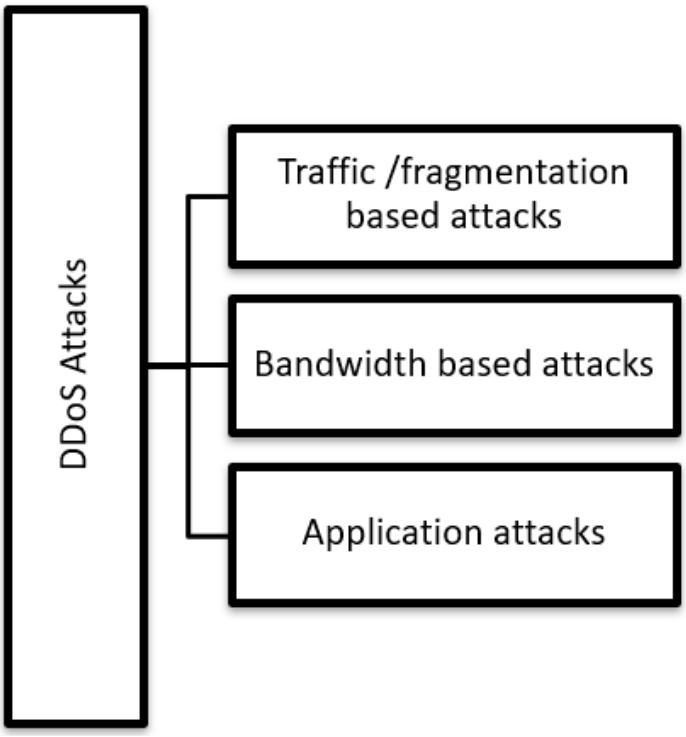

Figure 1. Classification of DDoS ((Distributed Denial of Service) attacks.

In general, a Denial of Service attack, which is usually called a DoS attack, is a purposeful attempt which is initiated so as to make an application or website unavailable to its legitimate users. This is achieved usually by flooding the website or application through network traffic. In order to achieve this, usually, one of the several choices of attackers is to apply diversified techniques that intentionally consume huge network bandwidth, thus causing inconvenience to legitimate users. Alternately, attackers also achieve this by handling system resources in an illegitimate manner. DoS attack is also called Non-distributed Directed attack wherein an attacker initiates DoS attack on the target system. The concept of DDoS attack is similar to DoS attack but the fundamental difference is that in DDoS attacks there are multiple attack sources which are implicitly involved, i.e., in DDoS attacks, the attacker makes an attack by using multiple sources which may include routers, IoT devices, and computers in a distributed environment infected by malware. To make this possible, an attacker looks for availability of any compromised network. By utilizing such compromised networks, an attacker usually attacks the target system through continuously generating packet floods or requests to conquer the target system. The DDoS attacks are common in the Network layer, Transport layer, Presentation and Application layer of the 7-layer OSI reference model. Network layer and Transport layer attacks are usually called Infrastructural attacks whereas the Presentation layer and Application layer attacks are commonly known as Application layer attacks.

2. Related Works

At an abstract level, one may view a DDoS attack as a clogged unexpected traffic on the highway so as to prevent the regular traffic flow arrival at its destination. DDoS attacks are usually performed through the use of a network of connected machines which are all connected via internet. The main problem with these types of attacks is the difficulty in discriminating between normal traffic and attack traffic as each Bot acts as if it is a legitimate one. DDoS attacks not only affect servers in distributed environments but also do not leave Cloud environments. DDoS attacks take the advantage of the services provided by Cloud environment such as (i) pay-as-you-go (ii) auto scaling and (iii) multi-tenancy. In a typical Cloud infrastructure, Virtual machines (VMs) are run in large numbers by Cloud servers to provide uninterrupted services to legitimate users of the Cloud environment. Now, in an event of an attack by attackers, the server can consider this situation as an event of higher resource utilization. The result would be the server trying to utilize an auto scaling feature in Cloud computing. The result of auto scaling feature could be allocation of resources, and migration of resources so as to solve the server overloading problem. Now, assume that resource allocation and process migration continues as a result of an attack, then, the attacker eventually becomes successful in DDoS attack that was initiated and that such an attack affects either directly or indirectly the Cloud services and eventually implicates the financial revenues. Some of the DDoS attacks in Cloud environment are Buffer overflow, SYN flooding, Ping of death, IP spoofing and land attack. DDoS attack defence in Cloud environments may be achieved by using three methods which include (i) Preventing attacks in the first place, (ii) Detecting the attacks and (iii) Mitigation of attacks. Anomaly detection and Botnet detection techniques are used for preventing and detecting a DDoS attack.

Denial of Service and Distributed Denial of Service attacks are the important sources that make internet services vulnerable. Attack detection is not new in using machine learning techniques. Some of the attacks that are identified though machine learning techniques are signature-based and anomalies-based. From ref. [1], it is learnt that signatures are used for signature-based Intrusion detection system, while detecting unknown attacks are the part of anomaly detection, whereas data flows generated by the unknown patterns gives the scope for studying DDoS. DDoS attacks can be prevented. Attacks are defined as violations of security policies of the network. Usually the attacks are classified into passive and active attacks. Passive attacks never affect the system but active attacks take control of system. The most frequent attacks in real-time network are Denial of Service (DoS) attacks. When a DoS attack is deployed into legitimate systems in a distributed environment, it is further considered as a Distributed Denial of Service (DDoS) attack. Distributed Denial of Service attack is where multiple systems try to target one single system. By flooding the messages to the target system, the services in the systems are denied and considered as zombies [1]. Some of the types of DDoS attacks are Flooding, IP Spoofing, TCP SYN Flood, PING Flood, UDP Flood, and Smurf attacks. Multiple machines are used to construct flooding in DDoS attacks.

- TCP SYN Flood attacks—The attack that spoofs the IP addresses is called TCP SYN Flood attack. This attack is more vulnerable as this is based on 3-way handshake protocol [2].
- PING Flood attacks—PING attacks are based on packets of ICMP request. As the PING attack targets the system, the connection slows down and reply request packets cannot be communicated from the end users.
- UDP Flood attacks—Target system cannot handle authorized connection once the threshold limit is reached. As the servers reach the threshold limits, the other packet requests are discarded.
- SMURF attacks—This attack occurred because of spoofed PING messages. By pinging the IP address, huge ICMP requests are received, further, more bandwidth will be consumed which slows down the computer to work.

The detections are divided into two steps: IP Entropy and Traffic collection module to extract entries and messages to detect DDoS attacks. Over the recent years, it has notified that many DDoS attacks incurred losses in heavy downtime, business loss, etc. One of the recent attacks where Amazon

EC2 Cloud servers attacked were by DDoS attacks [3]. The present hot topic across the area of research is to mitigate the DDoS attacks using machine learning techniques. Some of the recent works also have used Support Vector Machine technique to mitigate the DDoS [4]. Many machine learning methods like Naïve Bayes, SVM, and Decision trees were proposed to detect Distributed Denial of Service attacks. However, to detect this DDoS attacks using machine learning methods requires prerequisites on the network to identify the suitable data from the datasets [5,6]. Most of the common machine learning methods used in detecting the DDoS attacks are Convolutional Neural Networks [7], Long Short-term memory neural networks [8], Recurrent neural networks [9], etc. Over the years, the most widely used methods to detect Intrusion detection with DoS and DDoS attacks are based on machine learning algorithms. One such algorithm where the results were accurate and efficient in detecting the DDoS attack was using Decision Tree C4.5 algorithm [10]. Liao et al. [11] proposed a scheme based on SVM to detect the DDoS attacks using detection scheme base algorithm. Xiao et al. [12] proposed the most frequently used kNN algorithm for detecting the different types of anomalies in the network. By using the kNN algorithm, a maximum number of bots in the network were identified. Accuracy was improved compared to any algorithm in detecting the unknown attacks. In ref. [12], the author proposes a new method to detect the DDoS attack using Radial basis function (RBF) using neural networks algorithms. This RBF algorithm is used to classify the attacks as normal and abnormal. From the past study, it is identified that many clustering algorithms and a priori association algorithms are used to extract network traffics and packets [13,14]. Ref. [15] describes the detection of attacks using classification algorithms to monitor the incoming and outgoing packets in the network and also to compile the TCP SYN and ACK flags in the network. Ref. [16] used Artificial Neural networks to detect the DDoS attacks by comparing Decision Tree, Entropy, ANN and Bayesian algorithms. Further, in ref. [17], many researchers discovered that to detect different DDoS attacks, the separation of Flash Crowd event from Denial of Service attack is to be performed. One of the important approaches towards the DDoS attacks are SNORT and configurable firewall. Additionally, in ref. [18], it is shown that SNORT is used to reduce the false alarm rates to improve the accuracy in Intrusion prevention system. By having an impact on the real- time networks using Cloud Environment, the security services are blocked if the valid document is not used to detect intrusions. The proposed method in ref. [19] aims to detect DDoS attacks by statistical analysis of network traffic and Gaussian Naïve Bayes method is applied on training data for classification. The DDoS attacks are performed on various machines with two main methods. The first method is by sending the malformed packets to the victim and the second method is by performing either by exhausting the bandwidth or applying application level flooding [20]. In 2011, Lee et al. [21] proposed DoS attacks using Hadoop Framework. Ref. [21] used a counter-based detection algorithm to detect HR attacks using MapReduce algorithm. Many researchers have been using the Hadoop clusters in the Cloud computing platforms. Hadoop framework's job is only to monitor the data or packets. Many researchers have used the machine learning methods in order to create and view the DDoS attacks. Most often from the research, FireCol is the algorithm that is used to protect from flooding the DDoS attacks [22]. To detect the intrusion in DDoS attacks in the system, different classifiers like Ensemble reducing features, Heterogeneous and Homogeneous, are used for Ensemble methods [23]. Machine learning methods can also use to detect the DDoS in software-defined network. The study says that some of the issues were identified in the large network dataset for abnormal traffic using feature selection method to detect DDoS attacks. The most widely used approaches are feature ranking, scalability, and distributed approach.

3. Emerging Need for DDoS Attack Detection in Cloud Environments

The problem of DDoS attack prevention, detection and mitigation has received significant importance in relevance to Cloud computing environment. Of these three issues, the problem of DDoS attack detection has received primary importance from researchers. Researchers across the globe have been continuously working on proposing various methods and approaches to address detection of DDoS attacks. In spite of the availability of various contributions that addressed methods

and techniques to put a stop to DDoS attacks, unfortunately, even today the deployment of the available methods could not resist the DDoS attacks affecting the Cloud environments. In fact, they are substantially increasing over time interms of the frequency of attacks and also the attack size. One of the most common reasons is there is no consensus among various end points in a distributed internet network as one cannot enforce cooperation globally. The second reason could be the socioeconomic factors involved which makes the global cooperation enforcement difficult. The third point coins from the nature of DDoS attacks, i.e., there is no way of ensuring and enforcing a single point deployment so as to best ensure the defence against the DDoS attacks.

As per reports by Amazon Web Services, to date, the biggest DDoS attack that took place is in the month of February in the year 2020. The peak incoming traffic of this attack is seen to be 2.3 Tbps. The choice of attackers for making this attack was hijacked CLDAP webservers (Connection-less Lightweight Directory Access Protocol webservers) which is alternative to LDAP and is also a protocol used for handling user directories. Before this 2.3 Tbps DDoS attack in February of 2020, the second largest DDoS attack was the 1.3 Tbps DDoS attack—the one which targeted GitHub through sending 126.9 million traffic packets per second. Thus, there is an emerging immediate need to properly study, identify and figure out the reasons for failure of the available methods in the research literature.

4. DDoS Attack Detection Framework Using Multiple Linear Regression

The fundamental research objective behind the proposed method is to design a machine learning model based on multiple linear regression analysis and also perform data visualization by considering residual plots and fit charts. The idea behind the proposed approach is to study the possibility of applying multiple linear regression analysis to the CICIDS 2017 dataset which is the benchmark dataset widely used in some of the most significant recent research studies. The objective is to first apply the feature selection technique and determine the important attributes that are better deliverables for the prediction model. In the present approach shown in Figure 2, we have used the Information Gain approach method for carrying feature selection. Information Gain approach is a widely applied model in several data mining-based applications. The selected features are then considered for carrying multiple linear regression analysis, and the behavior of chosen and retained important attributes of the CICIDS 2017 dataset is studied by analyzing the fit charts and residual plots.The next subsection gives the experiment result analysis using the proposed approach by considering Friday log files of the most popular CICIDS 2017 research dataset.

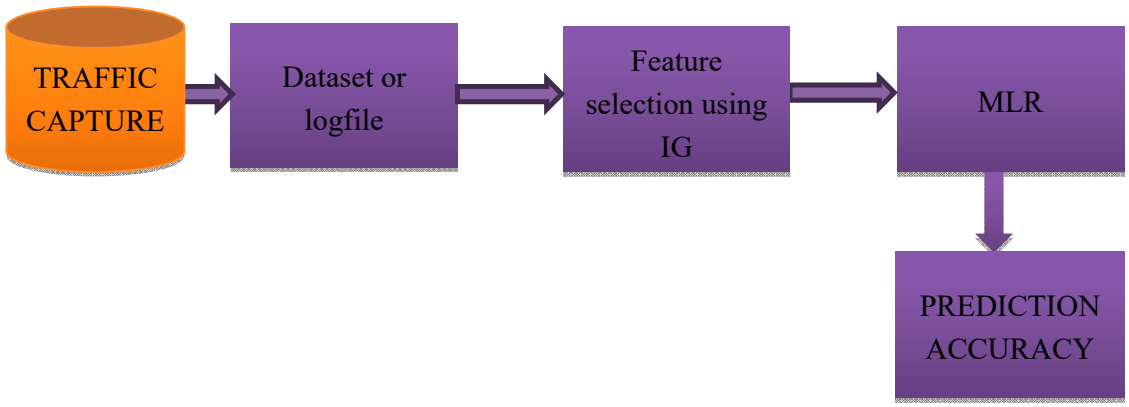

Figure 2. Proposed Machine Learning approach for DDoS attack detection.

5. Experiment Result Analysis

The dataset chosen for experimentation consisted of five-day log records from Monday to Friday in csv format. For experiment analysis, we have considered the log file of Friday afternoon which also consisted of two class labels. The class labels are Benign (Normal) and DDoS (attack). The total number of traffic packets in the log file included 225,746 traffic packets.

Experiment Analysis for the Log File of Friday Afternoon with Class Labels as Benign (Normal) and DDoS (Attack)

Initially, the number of attributes in the Friday afternoon logfile are 78 with the last attribute being the class label, i.e., there are 79 dimensions along with class label. Initially, the modeling process started by application of feature selection algorithm which is based on computation of information gain for each of the attributes in the dataset. The top 16 attributes have been considered for retention and other attributes in the attribute set are removed. Figure 3 depicts the entire details of ANOVA model and the list of the top 16 attributes with higher information gain are listed in Figure 4. For mathematical modeling, we chose to perform multiple linear regression analysis by running regression analysis on the logfile with these 16 attributes. After initial analysis is carried, the attributes that are retained include the attributes at dimensions 1, 5, 6, 7, 9, 11, 13, 35, 36, 53, 54, 55, 56, 64,66 and 67. The analysis is thus performed using the reduced dimensionality log file with these 16 attributes as mentioned above. The mean absolute percentage error for the linear regression model is obtained as 0.2621. Hence, the percentage accuracy of the multiple linear regression model is obtained as equal to 73.79%, i.e., 0.7379.

Figure 5 shows the residual plot obtained for each of the 16 attributes of the CICIDS 2017 dataset w.r.t Friday afternoon log file. Figure 6 shows the residual plot and Figure 7 shows the fit chart for the overall multiple linear regression model. After the initial model is developed, then, we have eliminated 10 attributes which are not statistically significant and retained the remaining sixattributes. So, the number of attributes is now reduced to sixattributes. The attribute dimensions are 1, 9, 13, 53, 54, and 64. Then, the multiple regression analysis is performed once again on these statistically significant attributes. Figure 8 depicts the fit chart, visualizing the actual label and predicted label. Figure 9 shows these six attributes' residual plots and finally, Figure 10 depicts the residual plot for the model. Thus, the machine learning model accuracy obtained using these six attributes is 71.6% which also clearly shows that the first model with 16 attributes is comparatively better.

ANOVA

	df	*SS*	*MS*	*F*	*Significance F*
Regression	16	29778.18946	1861.136841	23832.54328	0
Residual	225733	25640.72297	0.113588722		
Total	225749	55418.91243			

	Coefficients	*Standard Error*	*t Stat*	*P-value*	*Lower 95%*	*Upper 95%*	*Lower 95.0%*	*Upper 95.0%*
Intercept	1.480163181E0	1.214964E-3	1.218277377E3	0	1.477781883E0	1.48254448E0	1.477781883E0	1.48254448E0
Destination Port	-7.9586E-06	5.07513E-08	-1.568157955E2	0	-8.05807E-06	-7.85913E-06	-8.05807E-06	-7.85913E-06
Total Length of Fwd Packets	0	0	6.5535E4	#NUM!	0	0	0	0
Total Length of Bwd Packets	3.09845E-06	6.49544E-08	4.770183338E1	#NUM!	2.97114E-06	3.22576E-06	2.97114E-06	3.22576E-06
Fwd Packet Length Max	8.64604E-06	1.1702E-06	7.388505992E0	1.48996E-13	6.35248E-06	1.09396E-05	6.35248E-06	1.09396E-05
Fwd Packet Length Mean	0	0	6.5535E4	#NUM!	0	0	0	0
Bwd Packet Length Max	2.86673E-06	7.00377E-07	4.093126063E0	#NUM!	1.49401E-06	4.23945E-06	1.49401E-06	4.23945E-06
Bwd Packet Length Mean	7.06531E-05	3.26813E-06	2.161880723E1	1.5235E-103	6.42476E-05	7.70585E-05	6.42476E-05	7.70585E-05
Fwd Header Length	0	0	6.5535E4	#NUM!	0	0	0	0
Bwd Header Length	-5.97066E-4	5.71258E-06	-1.045177417E2	#NUM!	-6.08262E-4	-5.85869E-4	-6.08262E-4	-5.85869E-4
Average Packet Size	2.81867E-4	4.07743E-06	6.912847606E1	0	2.73875E-4	2.89858E-4	2.73875E-4	2.89858E-4
Avg Fwd Segment Size	-1.49379E-4	4.89145E-06	-3.053887974E1	2.0805E-204	-1.58966E-4	-1.39792E-4	-1.58966E-4	-1.39792E-4
Avg Bwd Segment Size	0	0	6.5535E4	#NUM!	0	0	0	0
Fwd Header Length	4.1925E-4	7.04326E-06	5.952493054E1	#NUM!	4.05445E-4	4.33054E-4	4.05445E-4	4.33054E-4
Subflow Fwd Bytes	-3.81369E-06	4.82535E-07	-7.903452827E0	2.72494E-15	-4.75944E-06	-2.86793E-06	-4.75944E-06	-2.86793E-06
Subflow Bwd Bytes	0	0	6.5535E4	#NUM!	0	0	0	0
Init_Win_bytes_forward	-1.24761E-05	9.91958E-08	-1.257727911E2	#NUM!	-1.26706E-05	-1.22817E-05	-1.26706E-05	-1.22817E-05

Figure 3. *p*-value and confidence intervals—ANOVA for CICIDS2017 Dataset.

S.NO	ATTRIBUTE NAME	INFORMATION GAIN	ATTRIBUTE DIMENSION IN CICIDS2017 DATASET
1	TotalLengthofFwdPackets	0.939343	5
2	SubflowFwdBytes	0.939343	64
3	AveragePacketSize	0.80995	53
4	TotalLengthofBwdPackets	0.782456	6
5	SubflowBwdBytes	0.782456	66
6	BwdPacketLengthMean	0.781841	13
7	AvgBwdSegmentSize	0.781841	55
8	forwardheaderLength	0.778016	56
9	forwardheaderLength1	0.778016	35
10	DestinationPort	0.77582	1
11	BwdPacketLengthMax	0.760317	11
12	Init_Win_bytes_forward	0.708411	67
13	AvgFwdSegmentSize	0.706064	54
14	FwdPacketLengthMean	0.706064	9
15	FwdPacketLengthMax	0.701009	7
16	BwdHeaderLength	0.682524	36

Figure 4. Attributes along with their information gains.

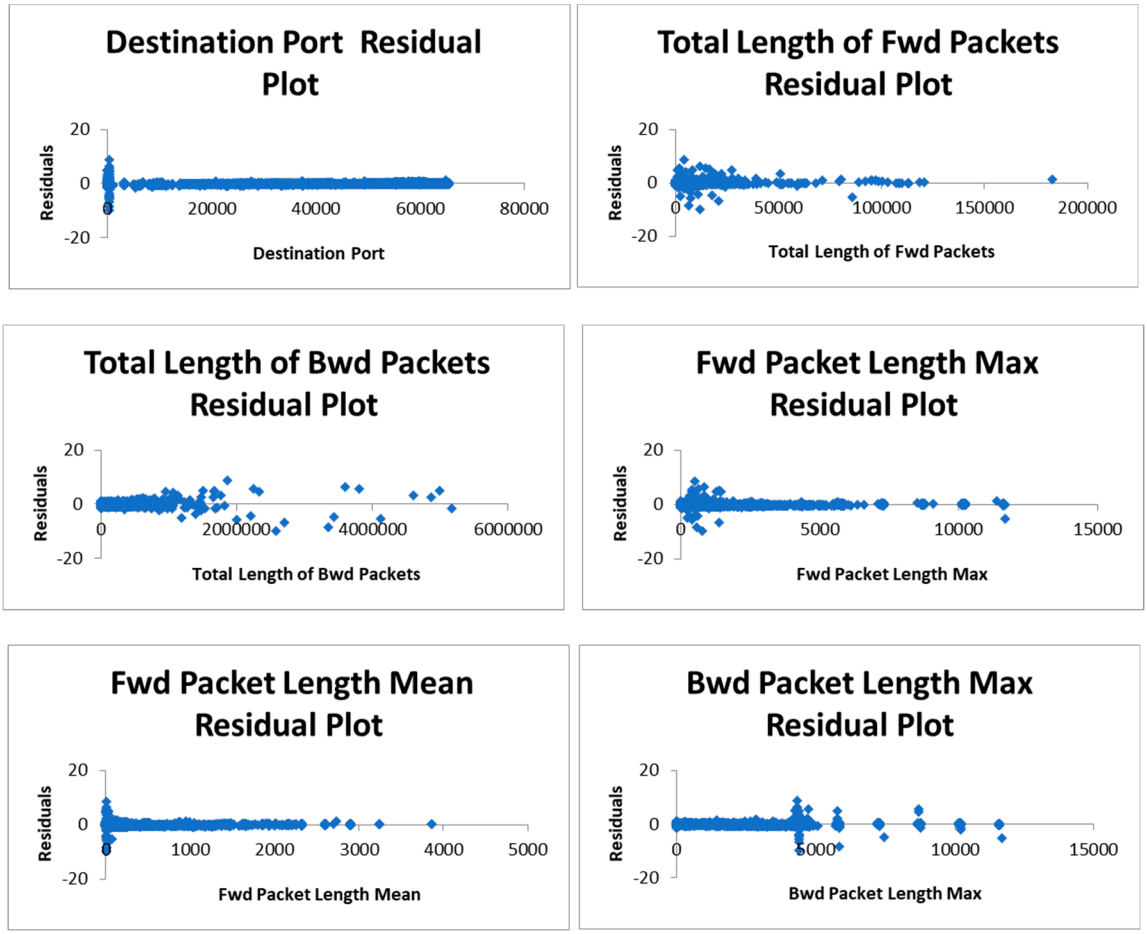

Figure 5. *Cont.*

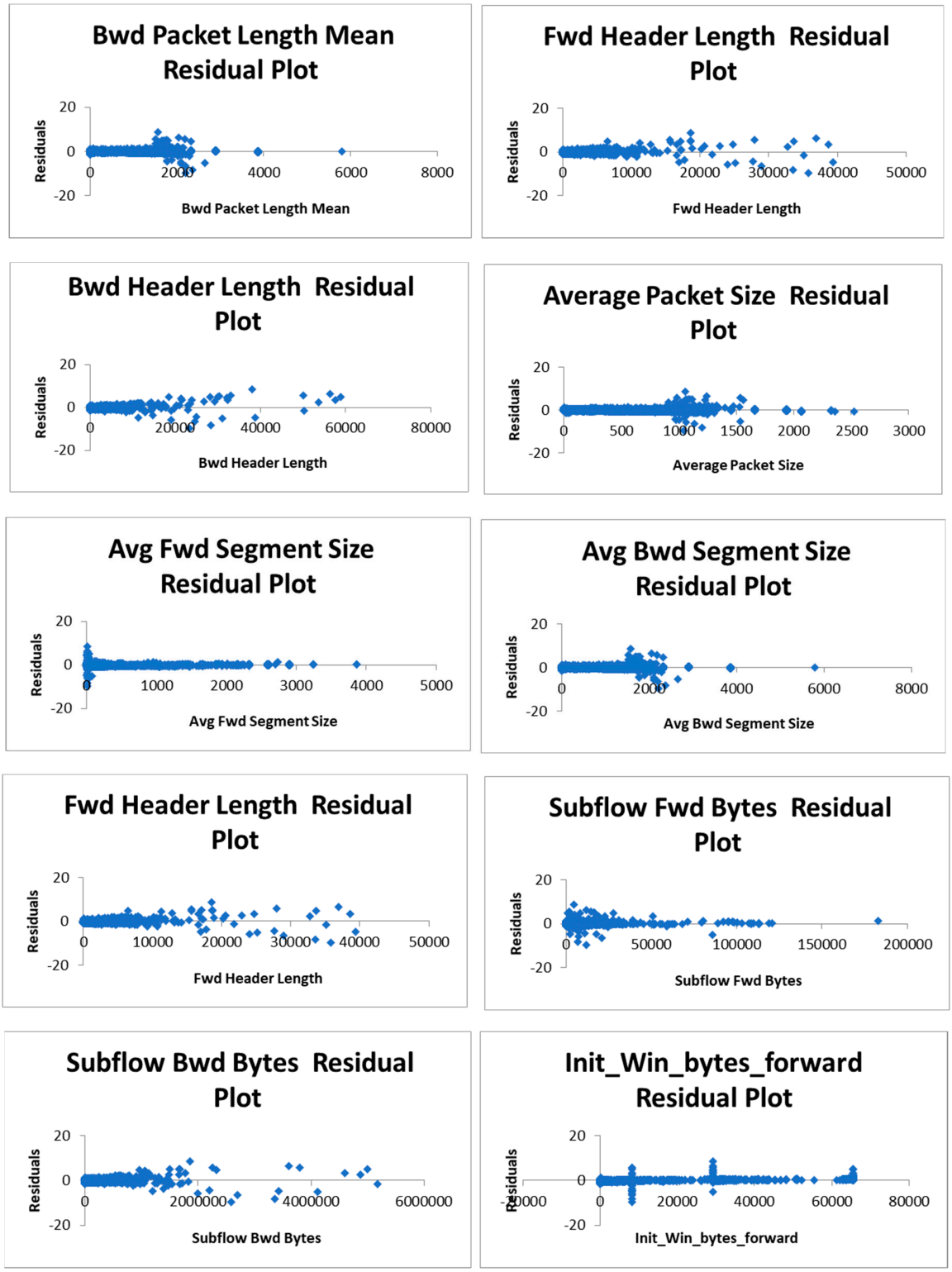

Figure 5. Residual plots for 16 attributes of Friday afternoon log of CICIDS 2017 dataset.

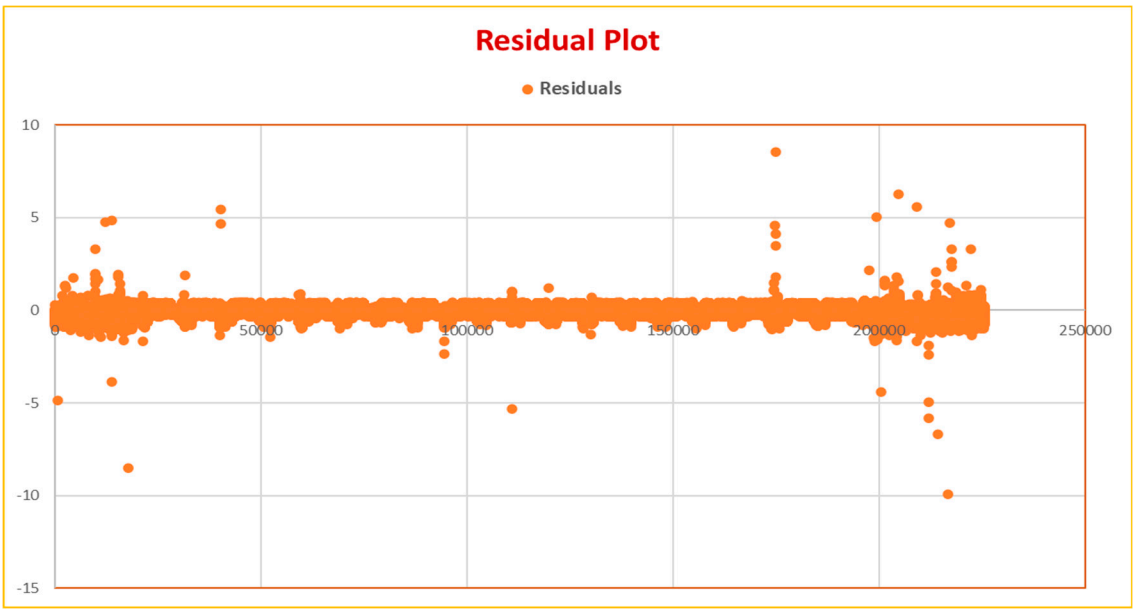

Figure 6. Residual plot obtained for multiple linear regression model for CICIDS 2017 dataset.

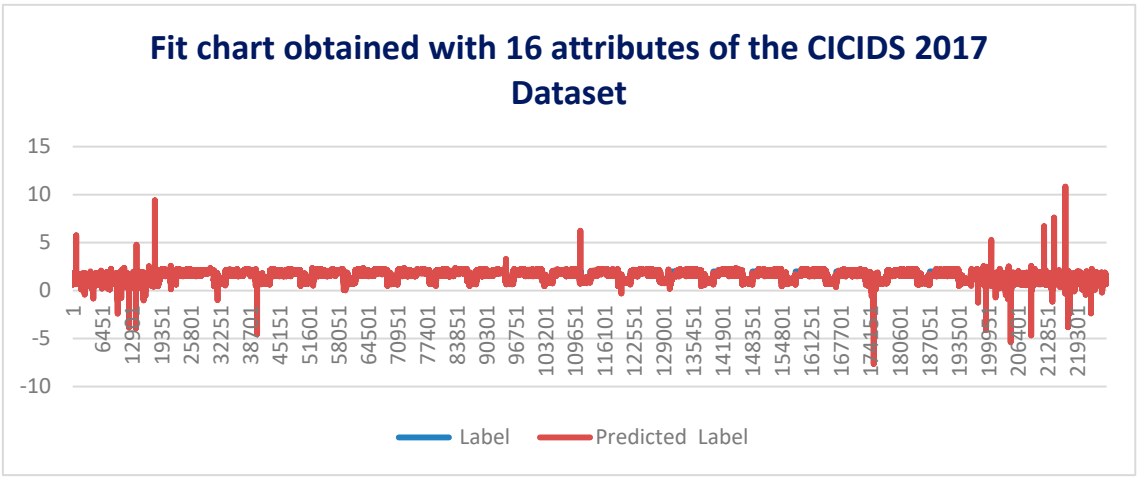

Figure 7. Fit chart obtained for Friday afternoon logfile of CICIDS 2017 dataset.

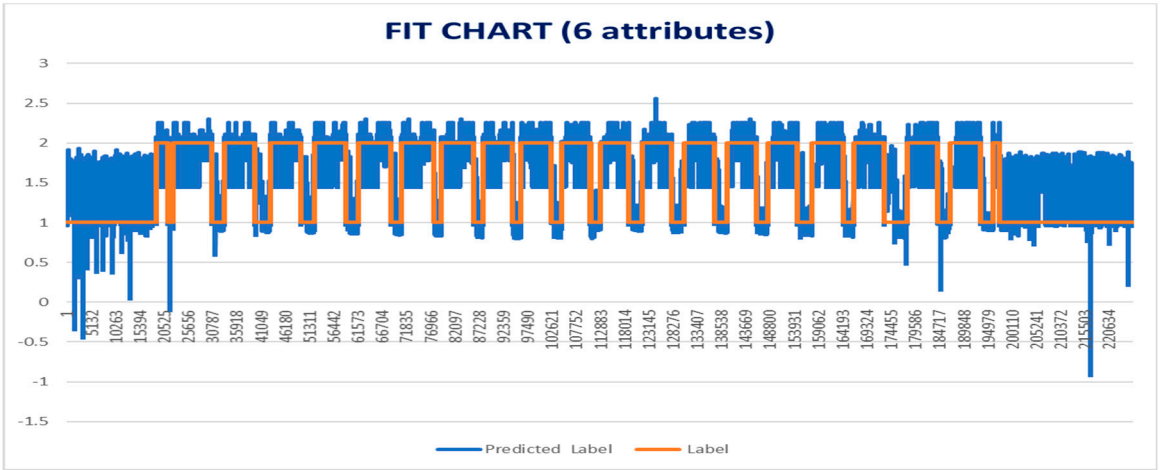

Figure 8. Fit chart obtained for Friday afternoon logfile of CICIDS 2017 dataset by considering 1, 9, 13, 53, 54, and 64 attributes.

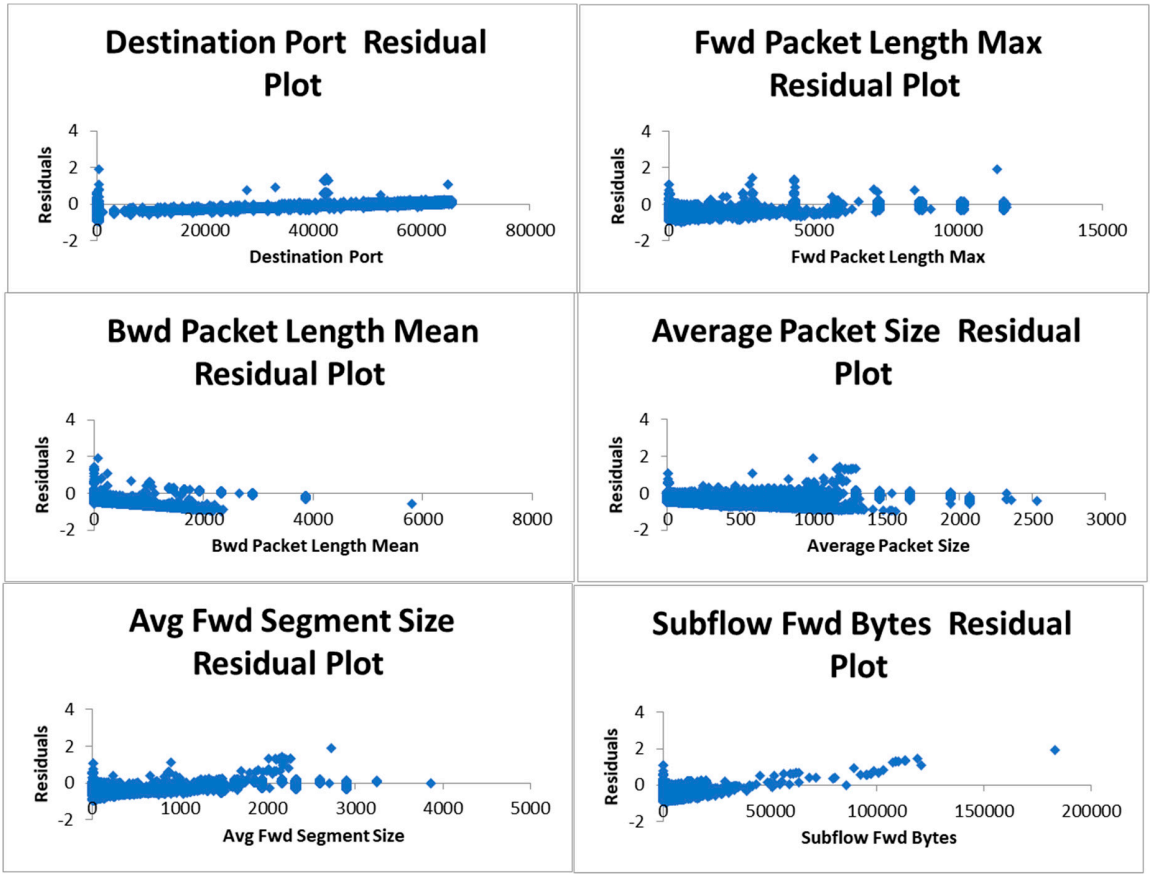

Figure 9. Residual plots for sixattributes of Friday afternoon log of CICIDS 2017 dataset.

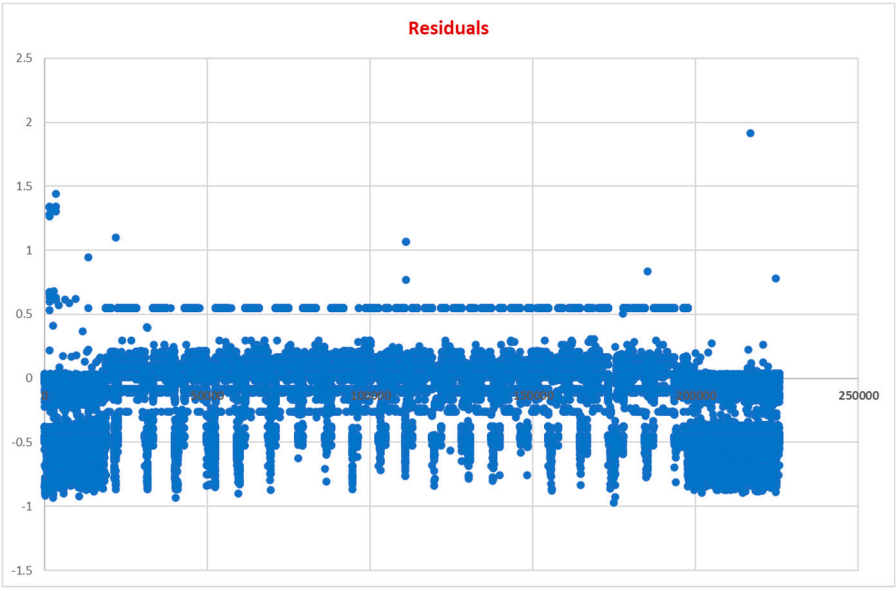

Figure 10. Residual plot obtained for multiple linear regression model for CICIDS 2017 dataset by considering six attributes of the dataset.

It can be seen from the experiment result analysis that the fit chart obtained by carrying multiple regression analysis on CICIDS 2017 dataset with the top 16 attributes obtained through information gain-based feature selection method is better than the fit chart obtained through considering sixattributes of the CICIDS 2017 dataset. This is because of the fact that in the later fit chart, the difference between

actual label and predicted label is clearly visible. Hence, the first model considered with 16 attributes is better for carrying the detection of DDoS attacks.

6. Conclusions

As detection of DDOS attack has become more common in a distributed environment like Cloud, it is essential to detect the attacks which cause service unavailability of Cloud. To identify such attacks, machine learning models can be used to train and test the attack detection datasets. Alternately, we can use the regression analysis technique by applying one of its important variants known as multiple linear regression analysis. The research objective behind this study is to build a machine learning model that is an ensemble of feature selection using information gain and regression analysis. For experimental study, the dataset considered was in the popularly known CICIDS 2017 dataset. Specifically, the Friday logfile of morning and afternoon are considered which has Benign, Bot and DDoS classes. It has been observed that through this ensemble model for Friday morning dataset, a prediction accuracy of 97.86% is achieved. Similarly, for the Friday afternoon log file, the prediction accuracy is obtained as 73.79% for 16 attributes obtained through information gain-based feature selection and regression analysis-based ML model. This paper thus paved a way to show the importance of regression analysis in building an ML model and also shows some of the important visualizations such as residual plots and fit chart which proves the importance of the model and its suitability of considering the model for prediction. In this work, we have limited our analysis for one-day log file and in future, this research may be extended to consider all traffic log files of fivedays and come out with a consensus-based machine learning model.

References

1. Dayanandam, G.; Reddy, E.S.; Babu, D.B. Regression algorithms for efficient detection and prediction of DDoS attacks. In Proceedings of the 2017 3rd International Conference on Applied and Theoretical Computing and Communication Technology (iCATccT), Tumkur, India, 21–23 December 2017; pp. 215–219. [CrossRef]
2. Sharma, N.; Mahajan, A.; Mansotra, V. Machine Learning Techniques Used in Detection of DOS Attacks: A Literature Review. *Int. J. Adv. Res. Comput. Sci. Softw. Eng.* **2016**, *6*, 100.
3. Somani, G.; Gaur, M.S.; Sanghi, D.; Conti, M.; Buyya, R. DDoS attacks in cloud computing: Issues, taxonomy, and future directions. *Comput. Commun.* **2017**, *107*, 30–48. [CrossRef]
4. Perera, P.; Tian, Y.-C.; Fidge, C.; Kelly, W. A Comparison of Supervised Machine Learning Algorithms for Classification of Communications Network Traffic. In *International Conference on Neural Information Processing*; Springer: Cham, Switzerland, 2017; pp. 445–454.
5. Zammit, D. A Machine Learning Based Approach for Intrusion Prevention Using Honeypot Interaction Patterns as Training Data. Bachelor's Thesis, University of Malta, Msida, Malta, 2016.
6. Doshi, R.; Apthorpe, N.; Feamster, N. Machine Learning DDoS Detection for Consumer Internet of Things Devices. *arXiv* **2018**, arXiv:1804.04159.
7. Hochreiter, S.; Schmidhuber, J. Long Short-Term Memory. *Neural Comput.* **1997**, *9*, 1735–1780. [CrossRef] [PubMed]
8. Chung, J.; Gulcehre, C.; Cho, K.; Bengio, Y. Empirical evaluation of gated recurrent neural networks on sequence modeling. In Proceedings of the NIPS 2014 Deep Learning and Representation Learning Workshop, Montreal, QC, Canada, 12 December 2014.
9. Breitenbacher, D.; Elovici, Y. N-BaIoT—Network-Based Detection of IoT Botnet Attacks Using Deep Autoencoders. *IEEE Pervasive Comput.* **2018**, *17*, 12–22.
10. Zekri, M.; El Kafhali, S.; Hanini, M.; Aboutabit, N. Mitigating Economic Denial of Sustainability Attacks to Secure Cloud Computing Environments. *Trans. Mach. Learn. Artif. Intell.* **2017**, *5*, 473–481. [CrossRef]
11. Liao, Q.; Li, H.; Kang, S.; Liu, C. Application layer DDoS attack detection using cluster with label based on sparse vector decomposition and rhythm matching. *Secur. Commun. Netw.* **2015**, *8*, 3111–3120. [CrossRef]
12. Xiao, P.; Qu, W.; Qi, H.; Li, Z. Detecting DDoS attacks against data center with correlation analysis. *Comput. Commun.* **2015**, *67*, 66–74. [CrossRef]

13. Karimazad, R.; Faraahi, A. An anomaly-based method for ddos attacks detection using rbf neural networks. In Proceedings of the International Conference on Network and Electronics Engineering, Hong Kong, China, 25–27 November 2011; pp. 16–18.
14. Zhong, R.; Yue, G. Ddos detection system based on data mining. In Proceedings of the 2nd International Symposium on Networking and Network Security, Jinggangshan, China, 2–4 April 2010; pp. 2–4.
15. Wu, Y.-C.; Tseng, H.-R.; Yang, W.; Jan, R.-H. Ddos detection and traceback with decision tree and grey relational analysis. *Int. J. Ad Hoc Ubiquitous Comput.* **2011**, *7*, 121–136. [CrossRef]
16. Li, H.; Liu, D. Research on intelligent intrusion prevention system based on Snort. In Proceedings of the International Conference on Computer, Mechatronics, Control and Electronic Engineering (CMCE), Changchun, China, 24–26 August 2010; Volume 1, pp. 251–253.
17. Chen, J.-H.; Zhong, M.; Chen, F.-J.; Zhang, A.-D. DDoS defense system with turing test and neural network. In Proceedings of the IEEE International Conference on Granular Computing (GrC), Hangzhou, China, 11–13 August 2012; pp. 38–43.
18. Ibrahim, L.M. Anomaly network intrusion detection system based on distributed time-delay neural network (dtdnn). *J. Eng. Sci. Technol.* **2010**, *5*, 457–471.
19. Fadil, A.; Riadi, I.; Aji, S. Review of Detection DDOS Attack Detection Using Naive Bayes Classifier for Network Forensics. *Bull. Electr. Eng. Inform.* **2017**, *6*, 140–148. [CrossRef]
20. Zargar, S.T.; Joshi, J.B.; Tipper, D. A Survey of Defense Mechanisms Against Distributed Denial of Service (DDoS) Flooding Attacks. *IEEE Commun. Surv. Tutor.* **2013**, *15*, 2046–2069. [CrossRef]
21. Gupta, B.B.; Misra, M.; Joshi, R.C. FVBA: A combined statistical approach for low rate degrading and high bandwidth disruptive DDoS attacks detection in ISP domain. *IEEE Int. Conf. Netw.* **2008**, 1–4. [CrossRef]
22. Francois, J.; Aib, I.; Boutaba, R. FireCol: A Collaborative Protection Network for the Detection of Flooding DDoS Attacks. *IEEE/ACM Trans. Netw.* **2012**, *20*, 1828–1841. [CrossRef]
23. Jia, B.; Huang, X.; Liu, R.; Ma, Y. A DDoS Attack Detection Method Based on Hybrid Heterogeneous Multiclassifier Ensemble Learning. *J. Electr. Comput. Eng.* **2017**, *2017*, 1–9. [CrossRef]