Network-based abnormal activity in a large data environment DDoS Attack Detection System

T.Kuppuraj[1*]

[1]Research Scholar in Computer Science, Department of Computer Science, Karpagam Academy of Higher Education, Coimbatore – 21

TKuppuraj66666@outlook.com

M.Mohan Kumar[2]

[2]Associate Professor, Department of Computer Science, Karpagam Academy of Higher Education, Coimbatore – 21

MMohanKumar452@outlook.com

Abstract

Distributed Denial of Service (DDoS) attack is a rising problem with rapid Internet growth. Times and low detection rates in the existing DDoS occurrence finding processes introduce a technique of identification of DDoS attacks based on abnormal network output in a big data environment. The method filters network flow based on the characteristics of a flood attack, permitting only the network flows, thereby minimizing intrusion from the usual grid flow and the accuracy detection. To represent changes in ancient and newfangled IP addresses for the many-to-one system flows, we set the Network-Based Abnormal Activity in Large Data (NBAALD). Finally, the NBAALD - based real-time DDoS attack detection method is developed to recognize the irregular network flow states of DDoS attacks. The consequences show approach has an established finding rate, a low false alarm rate, and an absent amount compared to similar procedures.

Keywords: Abnormal Activity, DDoS Attack, Detection system, network flow, Flood attack

1. INTRODUCTION

Most businesses, shopping, purchases, media, etc., in today's industry use the Internet online. The Internet is part of human being's daily life. Regular jobs are even more internet-dependent, but people still suffer from online fraud and cyber attacks. The most significant threat is the attack from the DDoS (distributed denial of service) (Chiba et al., 2019). Currently, the occurrence of the target attendant is carried out using human-made automated tools. A web-based Denial-of-Service (DoS) occurrence attacks the target web through legitimate or faulty requests. The server responds to the right regulars (Chiba et al., 2019). This form of CYB attack is mainly due to aggression, ransom, fighting, and political issue. The entire storage bandwidth is used, so the system has no reserves for processing the logical query. DDoS is a new formula for targeting DoS, as many occurrences come from various geographic areas directed at a single victim server. DDoS attacks in recent years display a growing increase in attack circulation that can exceed tens of GB or uniform hundreds of GB per second of the bandwidth of aggression (Sultana et al., 2019). It was

challenging to cope with conventional defensive tactics and mechanisms. In 2016, global IP traffic amounted to 1.2 dB a year, or 96 Exabyte's a month, allowing the Cisco Visual System table. By 2025, the global IP is expected to hit 3.3ZB or 278 Exabytes annually. Since network traffic is volatile and highly dynamic in the big data world, abnormal network behavior and a specific security approach are challenging in managing large-scale flood attacks (Yang et al., 2019). The increase in System Movement due to the high data surroundings, the features of serious difficulty, and the irregular performance of the network take remained challenging to deal with; a single method of defense is hard to deal with a significant flood attack and an effective defense mechanism (Wani et al., 2019). This paper suggests a flood occurrence detection approach built on irregular network activity in large data sets to address the above deficiencies.

A lot of detection and DDoS occurrence detection work has been conducted. A novel CAPTCHA (Fully Automated Public Turning Tester for Machine and Human Apart) or AYAH (Are you Human) page procedure founded on the calibration of user signatures has been provided (Gegan et al., 2020). The proposed approach produces a user signature and decides the user's behavior. The server's load is used to disable the AYAH page as a threshold (Habeeb et al., 2019). The method sends 1 AYAH page based on the signature of N requests. Therefore, using an AYAH page is inefficient, and the manipulators are unhappy with the CAPTCHA sheet's purpose.

The IBRL algorithm for the identification of DDoS attacks has been proposed. The approach considers the data transmitted from the advantage router to the object server at serial interfaces (Moustafa et al., 2019). The IBRL tests and associates the data output by the other edge router sequential borders. Suppose the first serial interface's throughput is higher than the other two, and its usage is over 95%. When it goes beyond this, the first interface must obtain the IBRL algorithm, and the same cycle continues for the rest of the system (Li et al., 2019). He primarily considers attacks on the network and layers of transport. However, a DDoS layer attack's impact on performance metrics cannot be differentiated from that of legitimate customers (Aghaei et al., 2019). The time it took to calculate the performance of the attack parameters would harm the victim's server (Jaber et al., 2020). A new way of detecting abnormal traffic based on chaos theory was proposed. A logarithmic procedure is used to pre-process circulation to deal with burst attack traffic (Dwivedi et al., 2020). For estimation of the traffic on the network, linear time series models like the Auto Regressive are used.

The results forecast is trained on neural networks and is used to detect any DDoS attack in the test data collection (Ujjain et al., 2019). Cases that are particularly prone to the initial state are technically subjected to anarchy (Selvakumar et al., 2019). During the attacking process, however, the DDoS parameters differ, and the initial state is less affected. When we wrongly believe the distribution, using time series models produces other errors (Zhu et al., 2019). The efficiency of the victim is rising, and the legal service customer notices that the victim is refusing service. Usually, a malformed packet is sent to the victim by an attacker (Xu et al., 2019). These products are assembled ignorantly for the program or a protocol on the victim's computer (Sharma et al., 2019). The delivery of these packages requires victims to freeze or restart the application or the

protocol (Cvitić et al., 2019). However, the characteristics of flood attacks are studied in this article. In this attack, the assailant sends much legitimate traffic to the victim's site.

It provides an early warning regarding the use of neural networks detecting DDoS attacks, and the method supplements the functioning of the traditional IDS (Alanazi et al., 2019). The article takes into account mounting detectors of anomalies at each topology node. That node tracks the position of both neighboring nodes and collects traffic analysis material for a skilled component. Furthermore, it involves creating a neural system through the correct participation and board information (Yusof et al., 2019). An inaccuracy in intelligence processing triggers a mistake in intruder detection. Detector placement in each topology node increases processing and maintenance costs. We suggest a calculated model of the DDoS occurrences and examine arithmetical limitations, such as the arrival of packs, to overcome the constraints of previous research (Jabez et al., 2019). The bandwidth and barrier scope of the attack is mathematically indicated.

The Model is a way of dividing and winning over the Network-Based Abnormal Activity in Large Data (NBAALD) idea. The principle of association and the usual possibility of circulation is more comfortable to apply to detecting attacks in clusters instead of the complete data set. The remaining element is organized as the corresponding work is introduced in Section 2. Section 3 describes the abnormal actions of the network—the experimental section 4. The conclusion is in Section 5.

2. DDoS attack on Network-Based Abnormal Activity in Large Data (NBAALD)

2.1. Data Processing

The address correlation (rating-ACD) and IP movement function were selected to prevent interference with the network flow multi-factored fusion, remove the one-to-one network movement interference produced by standard action, and increase recognition levels. The features are based on extracting features and characteristics (IP movement multi-feature, MFF synthesis), IP stream address semi-interactive anomaly degree (IP movement lecture, half communication irregularity notch, HIAD) as shown in Fig 1.

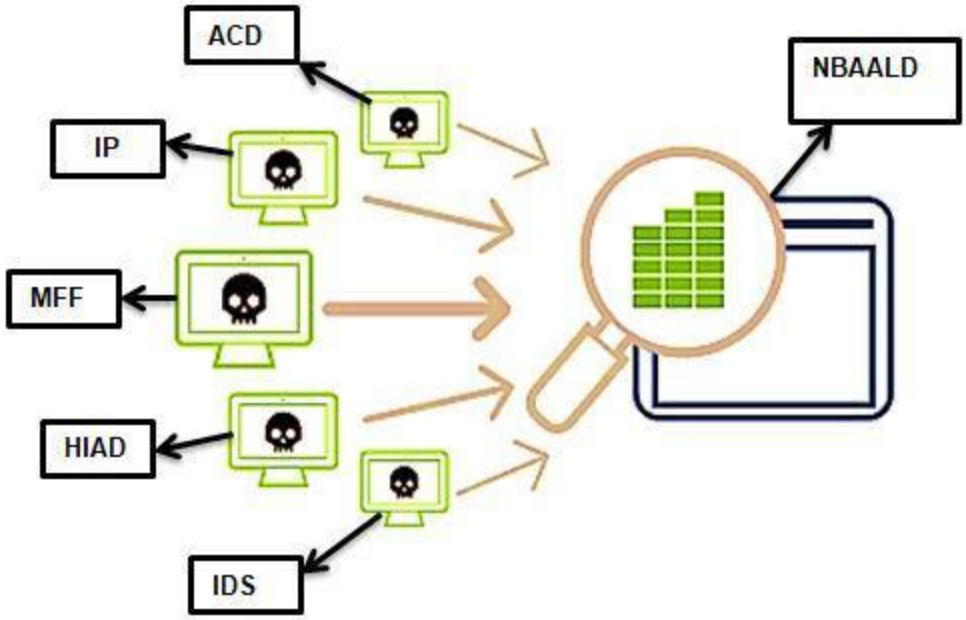

Fig 1: based on five methods of extracting features

A victim server attack by DDoS exhausts the target server's resources, which prevents new legitimate clients from connecting to a victim server. The storage resource expansion may be bandwidth or the defense side of the quarry storage. Equation (1) indicates the increasing likelihood of resource depletion after the survivor.

$$Total_{attack} = 1 - (1 - Q^{\propto})(1 - Q^{N}) \quad (1)$$

The attack model explains that bandwidth depletion and memory expansion are considered two separate cases.

2.2. Case A Bandwidth loss chance

The overall depletion of the victim's resources (bandwidth and memory) depends reverse on the rate of incoming customers.

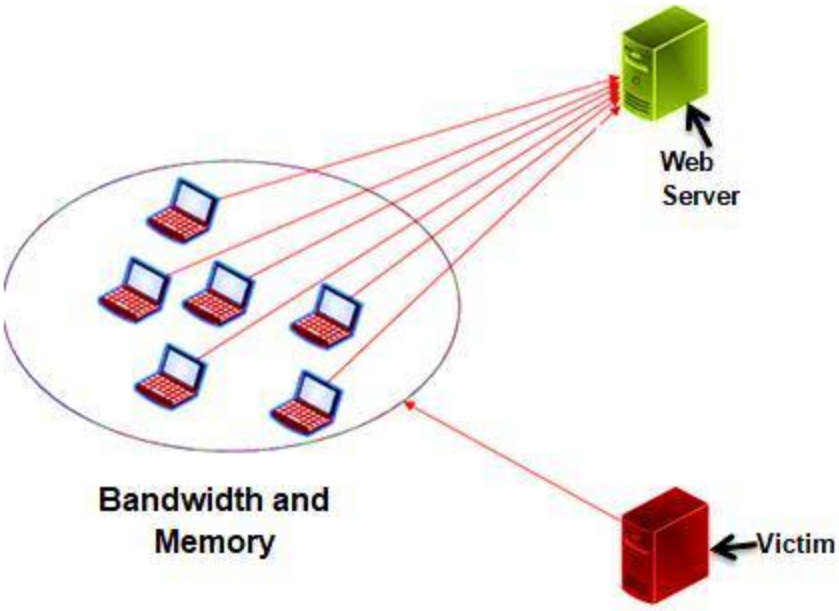

Fig 2: Bandwidth and Memory of NBAALD

The inference is that the less time between two delivery packages, the higher the probability of resource exhaustion, as shown in Fig 2. The time of inter-arrival and abnormality of the confronting packs. A higher price of the shield scope at the end of the victim determination hampers resource depletion. Furthermore, the increase in open channels also decreases the degradation of the bandwidth of the victims.

$$Total_{attack} = 1 - (1 - Q^{\propto})(1 - Q^{N}) \rightarrow Total_{attack} \rightarrow high \quad (2)$$

The amount of exposed networks and the defense scope of the object is limited if inter-income time is high, so Equation (2) is very likely to have complete exhaustion.

2.3. Case B

The probability of total explosion in Equation (3) is negligible if the intercom period is significant, the counter amount of networks open, and the cushion scope is excellent.

$$Total_{attack} \rightarrow Small \quad (3)$$

When the interval is short, and the available channel numbers lengthwise with the barrier scope are high, the possibility of complete fatigue is compromised due to equation 1. At least a specific time, the server will withstand the attack. Compared to cases A and B, the depletion rate of capital in the victim end is higher. This way, the target server will take a little longer to survive. Open

and memory channels are among the most critical requirements to avoid DDoS attacks as the first line of protection.

3. Extraction of Features

All network stream IP packets taken from a standard network stream V are referred to as J_m in unit time t. In compliance with the above rules, J_m is filtered. The category of filters is referred to as $G_m$as shown in Equation 4 and 5.

$$\nabla_{J_{mk}} \ni J_m \tag{4}$$

$$H_{J_n} \ni G_j \; if \; many \; to \; one \; network \; flow \tag{5}$$

Mark G_j as $P's$ IP addresses, all P "IP addresses are old users. If$m = 1$, $P'max = \max(P'\max \left\| G_j \cap P' \right\|)$ is the maximum user number. G_j It is merged with $P's$ after increasing unit time t to achieve the maximum amount of ancient IP numbers in the current unit time t as shown in Equation 6.

$$P'max = \begin{cases} G_1 & m = 1 \\ \max(P'\max \left\| G_j \cap P' \right\|) & \text{m} \geq 2 \end{cases} \tag{6}$$

New user number $O_m = \left\| G_j \right\|) - \left\| G_j \cap P' \right\|)$ Number of new users. The set "G_j" is the old user, "G_j" is the new user during the time, and E_j the number for new users during the period. The set "G_j" is the old user. The obtained parameter P'max indicates the maximum number of older users within the $-t$ timeframe while processing the standard network flow V which is the training sampleP'max. It is possible to measure the average amount of different users $\overline{M}$ for each part-time t as shown in Equation 7

$$\overline{M} = \frac{\sum_{j=1}^{m} O_j}{m} \tag{7}$$

For all sample capacity, we use a wordlist X_j to record the number of stays to any basis IP address SK through that historical using the similar element-time T to illustration the recognition stream W. $X_j = [T_{m,j}, P_{m,j}]$ For all the source IP addresses, we set the IP address in this paper over the k time so that the number of visitors to source IP X_j in the j period can be reflected. We measure four values in-unit time t, which are as follows an Equation 8,

$$NBAALD = -M \times B \times G \times T \tag{8}$$

To ensure precision, filter out all IP reports that comply with overflow features. The attached meaning defines the system.

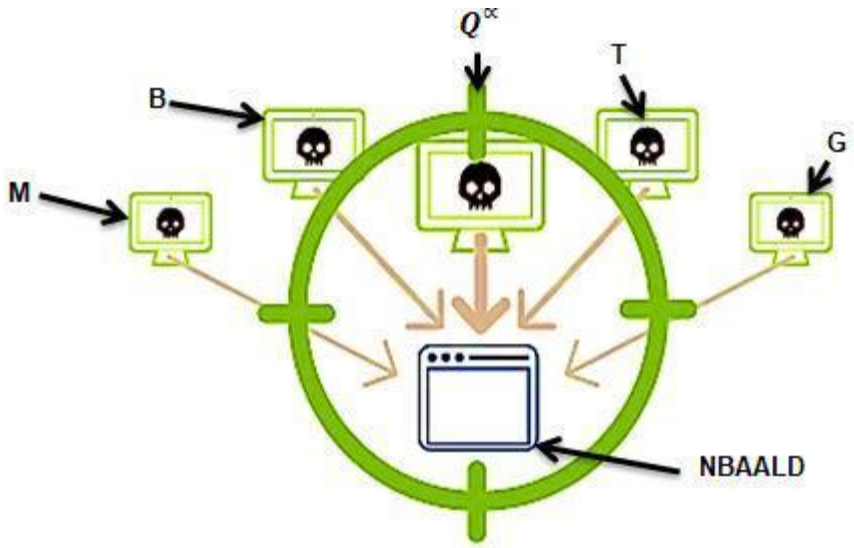

Fig 3 Extraction of Features of NBAALD

Flow norm. Older users = P is typically similar to the maximum value of $P'max$, which is around $\pm 0. P''max\ is\ almost\ 0$ as shown in Fig 3. Above the average value of the new user is the total number of unique users. As a consequence, the value B is nearly0. For F, additional old operators than new operators are available, and G is almost0. The Access Rate B_j is a small fixed value c for each user per second. Multiply by less the four. The final result is close to ± 0 as shown in Equation 9 and 10

$$M \to \pm 0, B \to 0, G \to +0, T = c \tag{9}$$

$$NBAALD = -M \times B \times G \times T \to \pm 0 \tag{10}$$

There may be limited access to sites for local users, in which the number of older operators may require a reduction. The P'' remains approximately -0. Five before bad or worse. 1. This situation prepares not to touch the last Model. However, then $B\ and\ G$ is near $0,$ as shown in Equation 11.

$$M \to -1, B \gg 1, G > 0, T \gg 1 \tag{11}$$

The total sum of new users \alter P' be much higher than the average worth of the innovative operator when the DDoS attack is conducted in DDoS, and the B value should increase. The website or network cannot deliver the facility to the old operator when the DDoS attack becomes successful. The total number of older users $\|G_j \cap P'\|$ And the value of the P' is nearly-1. The new user T has a broad access limit, as shown in Equation 12.

$$NBAALD = -M \times B \times G \times T\,'' + 1 \tag{12}$$

Furthermore, M is capable of reflecting the influence of DDoS occurrences on older operators, while NBAALD is used to quantify the effect of all-out attacks on DDoS.

Congestion of the network. Network congestion is another observable network flow. The number of new and old users will increase considerably when a hot topic emerges. There are three features: firstly, M should be very optimistic because of many new users; secondly, because the full range of hot subjects is likely to be accessible by the old users,t the value M should be above 1. Even if many new people live, the continual c would be a lesser value since it serves the usual users of the TCP / IP protocol.

$$NBAALD = -M \times B \times G \times T\,'' - 1 \tag{13}$$

Equation 13, G Refers to the degree to which external users are involved in a scorching topic. Since $Tm \ni (0,1)$ has a particularly searing issue, it may mean that elderly operators are troubled with the problem more.

3.1. Classification of NBAALD Method

Individual many-to-one network circulation is ported after the data collection has been filtered, which increases prediction accuracy. The trained ARIMA model is based on noiseless data and the fusion of its meaning. The time series $m = NBAALD, j = 1, 2$, after N cycles of the sampling and fuse of own values. And $P's$ earned. This paper model should be $ARIMA\,(3, 3, 2)$ by detecting the autocorrelation amount and the fractional self-correlation factor to the $ARIMA$ model parameter information criterion. This article usages second-order difference processing of raw $NBAALD$ statistics and displays the prediction and accurate data in Figure 4, well, and the ADF check, since the source data of this article is smooth. $ARIMA$ Model is set up in T-language.

The following paper uses a threshold-based network flow detector. The qualified $ARIMA$ Perfect was recycled for trend forecasting once the abnormal worth of $NBAALD$ was observed. The alarm is activated when continuous samples are above threshold value a. The threshold value$\beta = 34, \gamma = 4$, which means when two permanent anomalous sample points are present, is the experimental finding of this paper. A sliding window function with the nearest T locations is included in the $ARIMA$ trend prediction module. The number of abnormal $NBAALD$ values is defined in the $NBAALD$ points expected by the $ARIMA$ Model, and a DDoS alert is triggered if Ţ exceeds a certain percentage. Otherwise, the current network stream will be detected continuously until either $\gamma T\ is\ 0$ or the conditions have been encountered.

In the large data environment, DDoS attacks are only required quickly and accurately, but machine resources are also needed to circumvent or mitigate intrusion in standard network movement. In a large data environment, it is essential. In this paper, we establish a method for tendency forecast activation. In normal flow, the $ARIMA$ trend prediction module is inactive and

only activated after continuous irregular dots are detected. Finally, if the $ARIMA$ tendency forecast module decides that a DDoS occurrence is happening or the discontinue situation is being encountered, device-saving resources will be stopped.

The article uses standard network flows to create an IP address folder IPD for collecting older operators' IP addresses as training samples. The algorithm parameters and $ARIMA$ model parameters are generated simultaneously, and IPD is used to decide whether an IP statement is an old operator. The value of the attached article $NBAALD$ is calculated after every time t unit and forwarded as a sample point to the network flow recognizer. The identifier is α pre-set. The Sampling Point is marked as an outlier when the $NBAALD$ value of a sample argument exceeds β. Furthermore, the ARIMA module is started for pattern predictions when there are persistent γ outliers.

4. Experiment and Result Analysis

The length of a networking stream is 10 minutes; a networking stream starts at $14:50:37$, and the attack is about$15:16:60$, as defined in the CAIDA DDoS attack in the 2019 dataset. Therefore, monitor the start of a detection stream DDoS attack. $\nabla t = 1.2$ As the sample time of the test flow and measure the $NBAALD$ value.

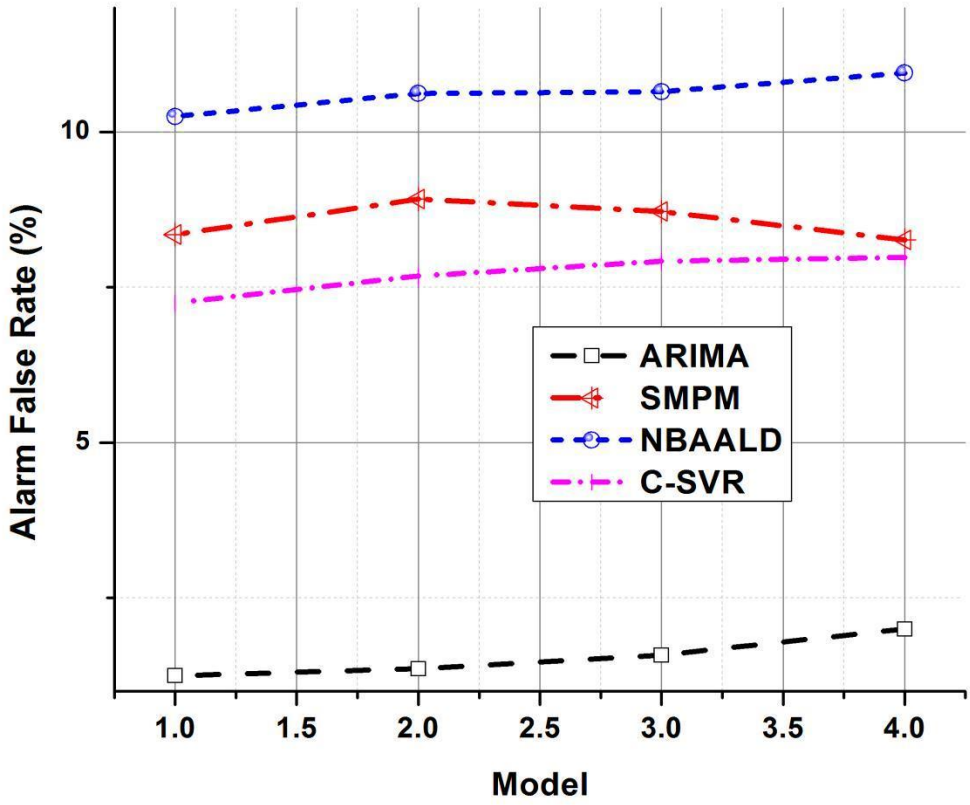

Fig 4 Models Vs. Alarm False Rate (%)

After analysis of the function values, variable N changes the most, and other variables obey. Variable N changes the most, as shown in Fig 4. The uneven weight of own fusion values is distributed as follows to help you better detect attacks:

$$NBAALD = -\tau_1 M \times \tau_2 B \times \tau_3 G \times \tau_4 T, \tau_1 + \tau_2 + \tau_3 + \tau_4 = 1 \quad (14)$$

Equation 14, Where, $\tau_1, \tau_2, \tau_3, \tau_4$ reflect weight by measurement of the critical component analysis of the four features,

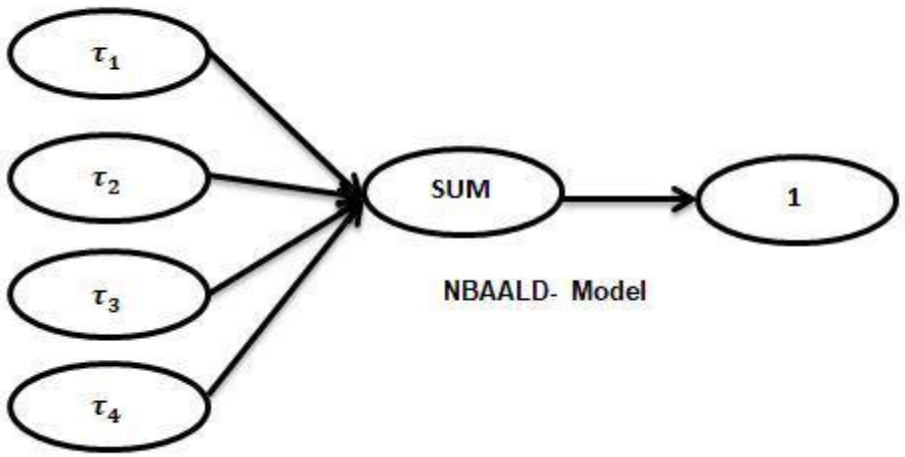

Fig 5 the variable weight of fusion of NBAALD-Model

This article defines TM as the amount of DDoS system stream illustrations correctly identified and FM as the standard stream number. Still, it is wrongly marked as a Net DoS stream, TQ is the number of users adequately recognized, and TM is the amount of DDoS system stream models incorrectly identified by standard stream models, as shown in Fig 5.

Equation 15, Detection rate DG. Specifies the classifier's ability to identify specific attack sources of DDoS.

$$DG = \frac{TM}{TM+FM} \tag{15}$$

Equation 16, MG. Suggests that the classifier might not be able to differentiate between actual DDoS attack streams.

$$MG = \frac{FM}{TM+FM} \tag{16}$$

Equation 17, Incorrect FG rate positive. Explain the possible classifier error for an average user to be identified as an attacker

$$FG = \frac{FQ}{TQ+FQ} \tag{17}$$

4.1. Analysis Based on the $NBAALD$ Model

ARIMA model is further used for prediction research, constructed on a secure preparation data set and the future fusion value NBAALD. There are also sample forecasts and future predictions showing reliable results. The test has been the data set CAIDA DDoS attack 2019, then the Model of training parameters are different$t = [0.05,0.10,0.5,0.9,2.4]$. First, to measure the network function values based on formula 10; furthermore, the original data movement for prediction. Second, to measure the system value conferring to Eq (16) for forecast and the cleaned data stream. Furthermore, both tests can differentiate average circulation from the DDoS flow.

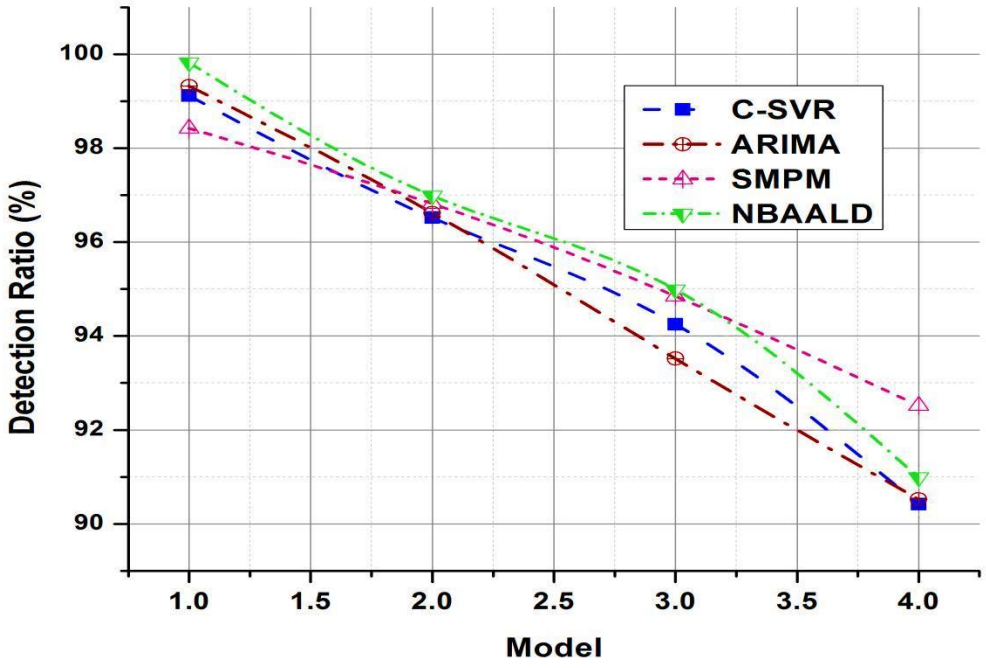

Fig 6 Model Vs. Detection Ratio (%)

A fake alarm will occur in the subsequent attack period when the sample time is short. If the sampling period is significant, the early attack time is illustrated by a false alarm. The characteristics and experimental data of the algorithm's future are analyzed, as shown in Fig 6. If t is high, even though the ARIMA model takes past data into account, new operators or a comparatively large amount of older operators in a small period, such a scenario would motionlessly lead to disappointment. If t is a large number of new operators and more former operators changing at the initial stage of the attack is small, leading to a false alarm.

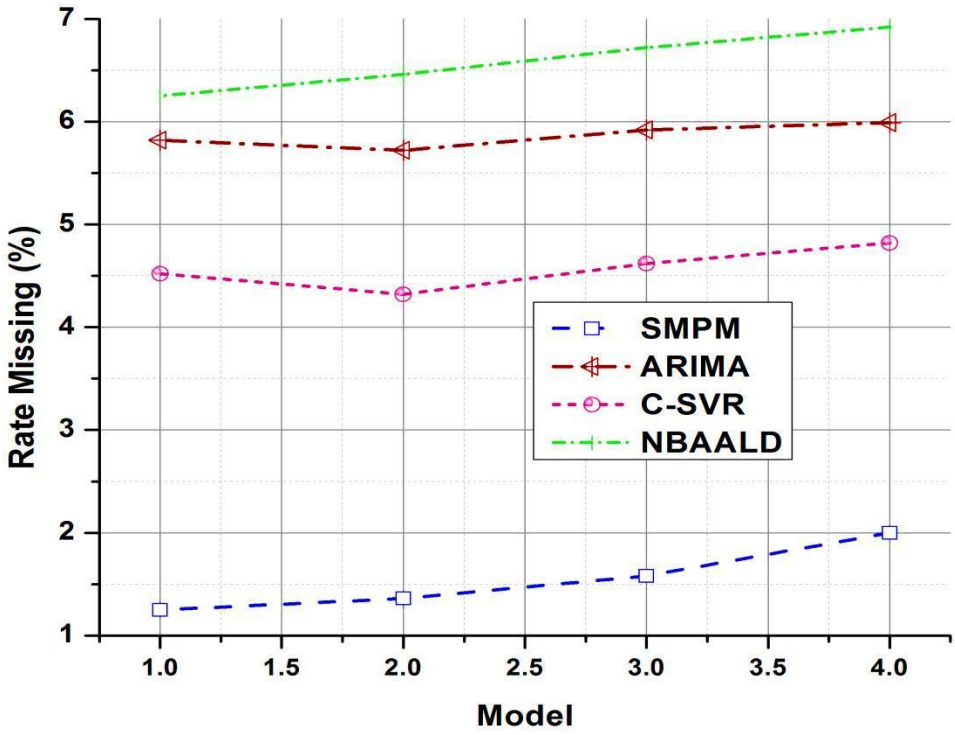

Fig 7 Model vs. Rate Missing (%)

Finally, we arrange cluster B inputs, i.e., time for the information and set the target 1 (attack) and cluster C information against the destination 0 (standard). The fitting function poly fit is then used to distinguish the difference, the training error, testing goals, and results. The convenient feature, as shown in Figure 5, is drawn by us using the Mat lab. Figure 6 presents the lined reversion plot of the total contribution to the goals provided later in the computational relationship. 98.68% of the fit between the data and the purpose can be achieved. The plot takes into account the blend of regular traffic and attack.

Table 1 Comparison of Model

Model	Detection ratio 1 (%)	Detection Ratio 2 (%)	Rate missing 1 (%)	Rate Missing 2 (%)	Alarm False Rate 1 (%)	Alarm False Rate 2 (%)
NBAALD	99.92	99.85	1.25	0.56	0.1	0
SMPM	96.12	95.62	5.82	3.48	8.35	6.35
ARIMA	94.26	93.68	4.52	1.89	10.23	7.52
C-SVR	90.38	91.27	6.25	8.67	7.25	4.125

This article contrasts the approach suggested with current plans, including SMPM, C-SVR, and ARIMA, as shown in Table 1. The test results of unfiltered network traffic detection using these methods are the detection ratio 1, the missing rate 1, and the false apprehension rate 1. The investigational results for the detection of clean network movement remain the detection ratio 2, the disappeared standard two and the incorrect alarm ratio 2. This paper defines TM as the number of correctly specified samples of DDoS network streams to determine the algorithm's effectiveness. FM is the number of regular streams mistakenly marked as a DDoS system stream. TQ has been a correct number of daily operators, and TM is the erroneously identified sample of DDoS system streams as standard stream examples.

5. CONCLUSION

This paper filters net traffic according to flux system movement characteristics, which decreases the above of the experiment and increases the precision of the finding of attacks. Furthermore, the NBAALD synthesis value is described as system IP statement change characteristics, and the movement is graded. However, NBAALD synthesis importance is described to define system IP report change characteristics, and progress is confidential. ARIMA prediction classic is developed based on NBAALD to identify DDoS attacks. Investigational findings show that the planned process is more accurate and valuable in detecting DDoS attacks than alternative methods. In the subsequent study, we will further explore how the current system can be combined with improved learning methods to increase detection accuracy. The approach is commonly used for the reimbursed creation of cloud robotics and intelligent cities.

Ethics Declarations

Conflict of interest

The authors declare that they have no conflict of interest.

Ethical approval

This article does not contain any studies with human participants or animals performed by any of the authors.

Author Statement

Conception and design of the study : T.Kuppuraj

Acquisition of data : M.Mohan Kumar

Analysis and/or interpretation of data : T.Kuppuraj

REFERENCE

1. Chiba Z, Abghour N, Moussaid K, Rida M. Intelligent approach to building a Deep Neural Network based IDS for cloud environment using a combination of machine learning algorithms. Computers & Security. 2019 Sep 1;86:291-317. https://doi.org/10.1016/j.cose.2019.06.013
2. Chiba Z, Abghour N, Moussaid K, El Omri A, Rida M. New Anomaly Network Intrusion Detection System in Cloud Environment Based on Optimized Back Propagation Neural Network Using Improved Genetic Algorithm. International Journal of Communication Networks and Information Security. 2019 Apr 1;11(1):61-84. DOI: 10.17762/ijcnis.v11i1.3764
3. Sultana N, Chilamkurti N, Peng W, Alhadad R. Survey on SDN-based network intrusion detection system using machine learning approaches. Peer-to-Peer Networking and Applications. 2019 Mar 1;12(2):493-501. https://doi.org/10.1007/s12083-017-0630-0
4. Yang C. Anomaly network traffic detection algorithm based on information entropy measurement under the cloud computing environment. Cluster Computing. 2019 Jul 1;22(4):8309-17. https://doi.org/10.1007/s10586-018-1755-5
5. Wani AR, Rana QP, Saxena U, Pandey N. Analysis and Detection of DDoS Attacks on Cloud Computing Environment using Machine Learning Techniques. In2019 Amity International Conference on Artificial Intelligence (AICAI) 2019 Feb 4 (pp. 870-875). IEEE. https://doi.org/10.1007/s10586-018-1755-5
6. Gegan R, Mao C, Ghosal D, Bishop M, Peisert S. Anomaly Detection for Science DMZs Using System Performance Data. In2020 International Conference on Computing, Networking and Communications (ICNC) 2020 Feb 17 (pp. 492-496). IEEE. DOI: 10.1109/ICNC47757.2020.9049695
7. Habeeb RA, Nasaruddin F, Gani A, Hashem IA, Ahmed E, Imran M. Real-time big data processing for anomaly detection: A Survey. International Journal of Information Management. 2019 Apr 1;45:289-307. DOI: 10.1016/j.ijinfomgt.2018.08.006
8. Moustafa N, Hu J, Slay J. A holistic review of Network Anomaly Detection Systems: A comprehensive survey. Journal of Network and Computer Applications. 2019 Feb 15;128:33-55. https://doi.org/10.1016/j.jnca.2018.12.006
9. Li D, Cai Z, Deng L, Yao X, Wang HH. Information security model of block chain based on intrusion sensing in the IoT environment. Cluster computing. 2019 Jan 16;22(1):451-68. https://doi.org/10.1007/s10586-018-2516-1
10. Aghaei E, Serpen G. Host-based anomaly detection using Eigentraces feature extraction and one-class classification on system call trace data. arXiv preprint arXiv:1911.11284. 2019 Nov 25. https://doi.org/10.48550/arXiv.1911.11284
11. Jaber AN, Rehman SU. FCM–SVM-based intrusion detection system for the cloud computing environment. Cluster Computing. 2020 Mar 25:1-1. https://doi.org/10.1007/s10586-020-03082-6

12. Dwivedi S, Vardhan M, Tripathi S, Shukla AK. Implementation of the adaptive scheme in evolutionary technique for anomaly-based intrusion detection. Evolutionary Intelligence. 2020 Mar;13(1):103-17. https://doi.org/10.1007/s12065-019-00293-8
13. Ujjan RM, Pervez Z, Dahal K, Bashir AK, Mumtaz R, González J. Towards sFlow and adaptive polling sampling for deep learning based DDoS detection in SDN. Future Generation Computer Systems. 2019 Nov 1. https://doi.org/10.1016/j.future.2019.10.015
14. Selvakumar B, Muneeswaran K. Firefly algorithm-based feature selection for network intrusion detection. Computers & Security. 2019 Mar 1;81:148-55. https://doi.org/10.1016/j.cose.2018.11.005
15. Zhu Z, Gu R, Pan C, Li Y, Zhu B, Li J. CPU and network traffic anomaly detection method for the cloud data center. InProceedings of the International Conference on Advanced Information Science and System 2019 Nov 15 (pp. 1-7). https://doi.org/10.1145/3373477.3373501
16. Xu R, Cheng J, Wang F, Tang X, Xu J. A DRDoS detection and defense method based on deep forest in the big data environment. Symmetry. 2019 Jan;11(1):78. https://doi.org/10.3390/sym11010078
17. Sharma P, Sengupta J, Suri PK. Survey of intrusion detection techniques and architectures in cloud computing. International Journal of High-Performance Computing and Networking. 2019;13(2):184-98. https://doi.org/10.1504/IJHPCN.2019.097510
18. Cvitić I, Peraković D, Periša M, Husnjak S. An Overview of Distributed Denial of Service Traffic Detection Approaches. Promet-Traffic&Transportation. 2019 Aug 10;31(4):453-64. https://doi.org/10.7307/ptt.v31i4.3082
19. Alanazi ST, Anbar M, Karuppayah S, Al-Ani AK, Sanjalawe YK. Detection techniques for DDoS attacks in a cloud environment. In Intelligent and Interactive Computing 2019 (pp. 337-354). Springer, Singapore. https://doi.org/10.1007/978-981-13-6031-2_34
20. Yusof AR, Udzir NI, Selamat A. Systematic literature review and taxonomy for DDoS attack detection and prediction. International Journal of Digital Enterprise Technology. 2019;1(3):292-315. DOI: 10.1504/IJDET.2019.10019068
21. Jabez J, Gowri S, Vigneshwari S, Mayan JA, Srinivasulu S. Anomaly detection using CFS subset and neural network with WEKA tools. Information and Communication Technology for Intelligent Systems 2019 (pp. 675-682). Springer, Singapore. https://doi.org/10.1007/978-981-13-1747-7_66