IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Survey about preventing the creation of zombie nodes for ddos attack in client server architecture using an intelligent algorithm

Dr.S.Hemalatha[1], Haritha.A[2] , Kanimozhi.S [3] , Kauvya Krishna Kumar [4]

[1] Professor, [2,3,4],Final Year /CSE , Panimalar Institute of Technology

ABSTRACT: ***DDOS have been significantly discussed in the computer security domain particularly due to damaging effect it causes to the organizational assets. There are many techniques to launch a DDOS attack such as UDP Flood attack, SQL Injection, Brute Force attack, Ping of death, SYN flood, Denial of sleep attack. Existing solutions can be divided into categories of machine learning solutions, distributed system solution or their combinations. The project proposes implementing automatic detection of attacks from the client side itself. Our concept is to identify the network traffic occurred by attackers through DDOS, SQL Injection and Bruce Force attack. We six different attacks which is made by attacker. 1) Request from Id with more number of time from within a time frame, 2) Request from same Id with different within short time, 3) Request from different Id , same request from different IP with multiple time, 4)Request from different Id, different request , different IP in a multiple time, 5) SQL injection 6) Brute force attack.This project mainly focuses on the zombie nodes detection and strictly eliminating them from the network.***

I.INTRODUCTION :

Of the several means for communication, most commonly used technology is the networking. The information is shared by the methodology of sending and receiving the request and response respectively in a FIFO manner. In this case, the server performance can be degraded due to multiple requests sent to the server by the clients. It may also happen due to the attack of Hackers. Websites become accessible to large number of users through internet, it may sometimes lead to overload of the server due to the maximum utilization. The result is server performance goes down and the processing time becomes slow. Due to the overload of the server, network traffic will be increased to corrupt server bandwidth.

DoS attacks are pernicious, a type of attack which checks on the availability of services and resources. It is an attack whose intention is to interrupt the normal traffic of a targeted server or a service. The request processing abilities of a server is exploited to process non-legitimate or rather unwanted requests from the attacker machine. Thus, the server/service is unavailable for the legitimate or rather the intended users. DoS attacks when occurs in a distributed environment is called DDoS. In DDoS scenario, the flooding non-legitimate requests come from multiple machines or systems which are in a disguised form. Thus recognizing, identifying such attacker systems and preventing them from further carrying out DDoS attack becomes a hectic, infeasible, time consuming, difficult task.

The targeted server of the DDoS attack is now burdened with an additional overhead of detecting these attacker nodes and then avoiding processing of requests from such attacker nodes. This consumes the CPU cycle and bandwidth of the server which is meant to be used for serving the legitimate and intended users. The intended

users or the admin will come to know that a DDoS attack has taken place only when one of the following occurs: (i) unusually slow network performance (response to requests, access to files, sites); (ii) unavailability of a particular web site. (ii) inability to access any web site. In general, DoS attacks are characterized or rather classified on basis of how they deny services: either by crashing services or by flooding services. Evidently the most dangerous attacks are distributed.

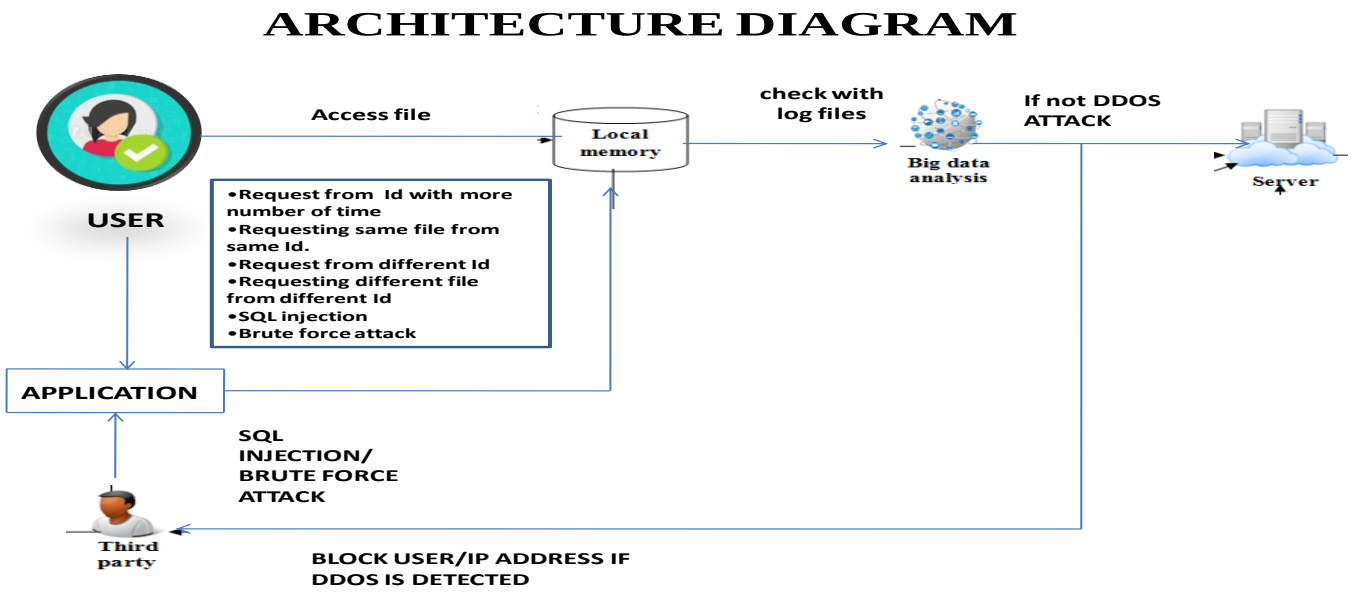
The immunity towards DDoS attacks is very minimal in all cases ranging from independent websites to multinational banks. In fact, a 2017 report from CisCo found that the number of DDoS attacks exceeding 1gigabit per second of traffic will rise to 3.1 million by 2021, i.e. a 2.5 fold increase from 2016. In most cases, DDoS attacks are designed merely to distract the target servers from criminal activities like data theft or network infiltration. That is the target is busy fighting off the DDoS attack, it then when the attacker would easily sneak in a piece of malware to carry out the criminal activity.

Several mechanisms are adopted by the large organizations and data centres. Still there cyber security efforts to mitigate the impact of these attacks are not up to the mark. The year of 2018 saw a slight decline in DDoS attacks. However, 2019 saw an 84% increase when compared tp 2018. This increase accounts to both the size and frequency of the DDoS attack. GitHub, a popular online code management service faced the biggest recorded DDoS attack. Its servers weren't prepared for the huge 1.3Tbps of traffic that flooded with 126.9 billion packets of data each second. GitHub used a DDoS mitigation service that was able to sense the DDoS strategy called memcaching. Dyn, one of the major DNS provider and a contributor of crucial part of the nework infrastructure of several companies like Netflix, Paypal, Visa, Amazon, had to face the most dangerous DDoS attack in October 2016. The hackers created massive botnets using a malware called Mirai to execute the DDoS operation. There are several other instances of many major companies which had to face the DDoS attack. The list includes BBC in Decemeber 2015, Spamhaus in March 2013, Bank of America in December 2012 and many more.

The DDoS mitigation strategies used up by the organizations or servers are all implemented on the server side. This is an extra burden for the server. Thus, we propose an intelligent algorithm which is to be programmed on the client side itself which monitors the request sent from its respective system, monitors whether it is a DDoS attack or a legitimate request and then sends he request to the server accordingly if needed. We propose that this algorithm should be incorporated at the OS level itself with hidden and unmodifiable properties such that the hackers or crackers will not be able to tamper on it. By client side, we mean each and every system that is being used by an individual which is capable of achieving services from a server. Various parameters like frequency of request issued, type of request issued will be considered by the intelligent algorithm to classify whether its host system is a DDoS attacker or a legitimate client.

A.ARCHITECTURE DIAGRAM:

Ssss



II. LITERATURE SURVEY :

A. Distributed Denial of Service Trin00, Tribe Flood Network, Tribe Flood Network 2000, And Stacheldraht.

Paul J. Criscuolo

A Denial of Service attack prevents the legitimate clients from enjoying the services they are authorized to. In summer of 1999, adding on to the traditional Denial of Service, the Distributed Denial of Service (DDoS) came into play. The DDoS employs several machines operating in harmony to attack a network, a site or a server and hence block the legitimate clients from accessing the network, site or server.
There were many tools developed to carry out the DDoS attacks. The first developed among them were Trin00 and Tribe Flood Network (TFN). These lead to the generation of next generation tools called Tribe Flood Network 2000 (TFN2K) and Stacheldraht. This paper includes the working of these DDoS tools, the mechanisms followed to detect them and their individual technical information. The DDoS attacks have become something difficult to track due to the cautious and superstitious capabilities built into these tools. Encryption is the key mechanism used by these tools to secure their communication and hide their source addresses. This makes it harder to detect these DDoS causing machines in the network. A small light on Network Ingress Filtering is also put in this paper. It is a method in which routers should be configured such that the outgoing packets are examined to ensure that source IP address belong to the subnet that the router services. This paper also talks about the tools that help in detecting the DDoS causing tools. The first such tool is the find_ddosv31 developed by the National Infrastructure Protection Centre (NIPC). This tool detects TFN2K client and its agent, Trin00 agent and its handler, TFN client and its rush-client and much more. Other such tools are ddos_scan and rid.This paper also tells about the various flood attacks involved in making the DDoS attack namely the ICMP flood attack, SYN flood attack, UDP flood attack, Smurf attack and the Targa3 attack. The ICMP flood attack or the ping flood is a common DoS attack where the victim's system is over rushes with excessive number of ICMP echo request which are otherwise called as pings. The Smurf attack is a DDoS attack which deals with spoofing the targeted victim's IP source address. A SYN flood is a type of DoS attack where a large number of SYN requests are sent in order to consume available network bandwidth or the server bandwidth.Thus this paper by Paul J Criscuolo is a study paper on what actually Denial of Service is, what does Distributed Denial of Service means, how they are perpetuated, what are the tools used for it, what are the tools used as a counter measure against the above mentioned tools and the various attack types involved in Dos and DDoS.

B. DeepDefense: Identifying DDoS attack via deep learning

X. Yuan, C. Li, and X. Li

According to this paper, the traditional or rather existing solutions to detect the DDoS attacks involve the use of machine learning techniques. The limitations in using machine learning techniques are that acquiring a data set and training the model based on the data set is quiet tedious. Moreover, the attackers come up with new attacking request types, such that a static data set becomes an infeasible solution to detecting DDoS attacks. This leads to the urge of a new method in which dynamic data set will be supported. In short, machine learning is a method to identify network activities based on statistical features and they are limited by the applications of only shallow representation models.Thus this paper proposes an approach called DeepDefense which is deep leaning based approach. The author states the reduction of error rate from about 7.5% to 2.1%. This approach manages to overcome all the limitations and shortages that were observed while using the machine learning techniques. The frequent overhead of updating the model, and setting the accurate threshold value is given a solution through this paper. The DeepDefense approach is used to detect DDoS attack at the victim's end and eliminate all above mentioned issues. The data set used in this approach is the UNB ISCX Intrusion Detection Evaluation 2012 Data Set. The key factor to be noted is that the size of the data set is very large. When comparing the performance rates of many neural network models in various domains, it is observed that the Gated Recurrent Unit Neural Network (GRU), Convolutional Neural Network (CNN), Long Short Term Memory Neural Network (LSTM) and Recurrent Neural Network (RNN) have very good performance rates and

hence the DeepDefense makes use of these models.The proposed method's main aim is to naturally fit the dynamically varying data sets into our models. The neural models are trained so as to understand the subtle difference between DDoS traffic and the legitimate traffic. This makes it necessary to feed the model with historical information as well. RNN is used as it has the advantage of independence from the size of window of the input. Therefore it can detect any type of DDoS attack, no matter old or new. The CNN model is adopted to obtain knowledge about the local correlations among network fields.The various attacks checked during the experiment time of this propose approach are IMAP attack, flowgen attack, HTTPWeb attack, Unknown_TCP attack, ICMP flood attack, Secure Web attack and MiscApplication attack on Data14. The various attacks checked during the experiment time of this propose approach are Secure Web attack, SMTP, DNS, HTTPWeb, IRC and Unknown_TCP on Data15. The experiments evidently make it clear that it does not have any dependence on the window size. The error rate is reduced by 39.7% in Data14 and by 5.4% in Data15.This paper also focuses on to increase the DDoS vectors included presently and consider many more factors that might affect the robust nature of the model in different environments. The paper also makes a clear understanding about the need for creation of new data sets.

C. Real-time anomaly traffic monitoring based on dynamic K-NN cumulative-distance abnormal detection algorithm.

R. Song and F. Liu

This paper has been referred as it gave an idea on live anomaly traffic monitoring. Due to the rapid growth of mobile internet and its wide scalability features, the number of users on the internet increases double fold. This makes it necessary to monitor the activities taking place on the internet and keep track of all suspicious activities. It is to be noted that suspicious activities here means the abnormal flow of packets which leads to DDoS attacks and affects the legitimate users from enjoying the services they need. This paper proposes a new methodology for detecting anomalies on huge traffic data. The number of such studies that encounter anomalies in the real time are not up to the mark. This paper proposes a dynamic K-NN cumulative-distance abnormal detection technique algorithm.This algorithm makes use of the Storm technology. The monitoring of network traffic and its anomalies is essential for network operators for many tasks like network maintenance, log analysis and ensuring security. The existing solution is based on transform domain which deals with transformation of signal from time domain to frequency domain. Then based on some pre-described features, anomalies, if any, are detected. The impracticality of this method lies in the fact that it is quiet complex and not adoptable in the real-time scenarios. Also some studies made use of the Hurst parameter to detect anomalies. The Hurst parameter is the best suited when network is busy, but then self-similarity parameter becomes weak.This paper mainly focuses on the increasing number of smart phone users and enlightens the fact that internet especially mobile internet has taken the facet of Big Data. If Big Data then Hadoop is the normal implementation technique we choose. Then, if Hadoop is chosen, HDFS comes to play. This leads to distributed processing which contradicts our requirement. This is whey Storm processing is used. This Storm technology manages to cover the three aspects: real-time data, huge volume of data processing and analysis technology. The Storm technology is a distributed processing system that divides the work and assigns simple yet specific tasks to different components. The processing of input stream is done by Spout component and further processing by required number of Bolt nodes. The modules specified in this paper are monitor module, top-N module, storage module and the query module. It is the query module that figures out the anomalies in the network traffic. The experimental setup used 6 worker nodes of same configurations and data set was developed by Traffic Monitor System (TMS). The authors strictly claim that this proposed method is a perfect solution for detecting anomalies in the network traffic.

D. Efficacy of live DDoS detection with Hadoop.

S. Hameed and U. Ali

This paper speaks about an efficient detection method to detect live DDoS attacks with help of Hadoop. If we incur an delay in detecting such attacks, then the only solution left out will be to manually disconnect the target system and fix the issue. It is found that the increase in internet traffic every year is doubled and hence

monitoring the network traffic to identify DDoS attacks is definitely a challenging task. This paper concentrates on TCP-SYN, HHTP-GET, UDP and ICMP flooding attacks and takes necessary countermeasures against them. Due to increase in internet traffic, real time anomaly detection with Snort and Bro Intrusion Detection Systems have become a bottleneck. A similar solution to the proposed solution, stated by Lee et al, used a Hadoop based model and counter based MapReduce DDoS algorithm. But it was limited to be used only for offline batch processing of huge volume of traces.

This paper proposes HADEC which is a Hadoop based live DDoS Detection framework. The idea of HADEC is novel that makes use of Hadoop to detect live DDoS attacks. The two main components of HADEC are the capturing server and the detection server. The capturing server is responsible for capturing the live updates of network traffic. The detection server contains the algorithm to specifically detect the DDoS attacks from the network traffic that was captured by the capturing server. The four main phases of HADEC are implemented via separate components. They are: i)network traffic capturing and log generation ii)log transfer iii)DDoS detection and iv)result notification. It is keenly observed that the key performance overhead of HADEC is used to capturing of live network traffic and in worst case scenarios it accounts to 77% of overall detection time.

E. Distributed denial of services attack protection system with genetic algorithms on Hadoop cluster computing framework.

M. Mizukoshi and M. Munetom

DDoS has become one of the menaces of Internet security. Identification of such attacks have become very difficult due to the attacker sending spoofed packets to the victim. Pattern matching and other similar techniques are not a complete solution to DDoS because each and every time the attacker finds out a new way to impose DDoS on the victim clients. Thus, there comes a need to find out a dynamic solution which will be able to find any type of DDoS, no matter old or new.

This paper proposes a highly scalable, a real time suitable traffic pattern analysis based on genetic algorithm which helps in detection and prevention of DDoS attacks on Hadoop infrastructure. It proposes a host side DDoS prevention scheme which uses above mentioned genetic algorithm on Hadoop MapReduce framework. The information about recognition of packets and their arrival patterns is used to generate a filtering rule which in turn is used in host side DDoS detection. The two major issues of scalability and adaptation to continuously changing DDoS attack patterns is easily covered up by the genetic algorithms implemented on Hadoop MapReduce framework.

The previous works on network traffic analysis were dealt by using Hadoop 1.0 which performed offline analysis on information regarding packet size, their source IP addresses and frequency of communication while the proposed system uses Hadoop 2.0 which has the characteristic of process streaming and iterative processing. The three major modules of this proposed solution includes (a)packet profiling with genetic algorithm (b)entropy based DDoS detection and (c)DDoS filtering rule base. The experiment results stated in this paper assures effective detection of DDoS attacks with high accuracy.

F. Understanding botclouds from a system perspective: A principal component analysis.

H. Badis, G. Doyen, and R. Khatoun

Cloud computing is known for its on-demand, reliable, elastic availability of computing resources, storage resources and various other powers. This fast leveraging power of cloud computing is exploited by the malicious attackers to cause DDoS attacks. Among them Botnets are the greatest beneficiaries. In an highly dynamic and heterogeneous environment like cloud, it is quiet challenging to dtect and prevent such type of attacks. Features like on-demand service, elasticity, reduced infrastructure and operational costs, pay-as-you-go model are some factors that make clod computing popular and widely used. It is to be noted all above mentioned features are offered ensuring scalability.

This paper states the results of an experimental campaign that was conducted in order to infer the operational behaviour of a botclouds used for a DDoS attack. The novelty here lies in the system metrics considered. Attacks based on TCP flood and UDP storm are considered for this experimental campaign. The result of this campaign highlights the peculiar behaviour of a botclouds when compared to other legitimate worker nodes.

The experimental set up discussed here considered the following two hypothesis: (a) it is only possible to monitor activity of subset of servers of data centres. Therefore security is bounded at the physical layer. (b) To maintain privacy of clients activities, the sole metrics available at hypervisor level are limited. Thus the metrics considered here are: CPU, Bandwidth send, Bandwidth received, Memory. The experiment is conducted in three phases. Each phase is said to last for an hour. In the first phase the botclouds is deployed but it does not affect any victim clients. The second phase involves the attack towards a third party. In the third phase, the DDoS attack is halted and the system is brought back to normal state. This paper needs further studies to be made on (i) the comparison of the botclouds activities with all legitimate worker nodes (ii) developing a distributed source based detection technique for botcloud's DDoS attacks (iii) developing self-protection system for cloud service providers against DDoS attacks.

G. A deep learning approach for intrusion detection using recurrent neural networks.

C. Yin, Y. Zhu, J. Fei, and X. He

An intrusion detection system is a system which checks on various illegal attacks and accesses in the network. Intrusion detection is thus an important security aspect in the Internet network. A key technology is essential that would accurately tackle various attacks in the network.
This paper has undergone an exploration on how to develop an intrusion detection model based on deep learning. This paper proposes an intrusion detection system that uses deep learning approach using recurrent neural networks. A study is also made on the performance of the model on binary and multiclass classification, based on number of neurons, impacts based on different learning rate. The study is then compared with various machine learning methods like J48, random forest, support vector machine, artificial neural networks. The experiment results makes it evident that recurrent neural network intrusion detection system works in a superior way when compared to the existing or rather traditional machine learning methods.

H. Discriminating DDoS attack traffic from flash crowds on Internet threat monitors (ITM) using entropy variations .

K. M. Prasad, A. R. M. Reddy, and K. V. Rao

Internet threat Monitoring (ITM) is found to be a monitoring system in the internet to detect and to measure the security attacks against sources of attack. Distributed Denial of Service (DDoS) was found to be a serious threat to the internet earlier.It was found that attacker uses botnets to launch DDoS attack by sending high traffic in network and the goal was to exhaust ITM network resources i.e computing power of victim system, data structures used in victim operating systems. The attackers here attempts to disable the ITMs by sending heavy traffic in the pattern of flash crown. The Flash Crowd flows are from legitimate users and they are found to be normal requests and the generated outputs were found to be similar with the effect of DDoS attacks.So, it is important to distinguish DDoS attack flows from flash crowd flows in the heavy traffic, for those who prevent against DDoS attacks. It was found that, use of a discrimination algorithm based on entropy variations as a similarity metric was effective among suspicious flows. Formulating the problem in the internet with botnets, has presented theoretical proofs for the feasibility of the above proposed method. So in this method, it has defined a way to detect the internal and external attacks in internet at ITM monitors performed by an attacker using botnets. They have used entropy variations to vary the signals and to discriminate the flash crowd attacks from legitimate flash crowds. It was theoretically proved that the possibility of the proposed detection method, was effective at ITMs. This entropy variations approach was used to identify the legitimate flash crowd but with the help of threshold value that was obtained helps to identify the traffic depending on the size of the network traffic.

I. Deep Learning Approach for Network Intrusion Detection in Software Defined Networking.

Tuan A Tang , Lotfi Mhamdi , Des McLernon , Syed Ali Raza Zaidi and Mounir Ghogho

Traditionally, in this paper there were found to be two types of NIDS according to strategies to detect attacks in network traffic. The first one, was detection based on signatures, comparing it with new set of data with already known knowledge base intrusions. Though there is a fact that this method cannot recognize new types of attacks,still it is found to remain the most popular approach in commercial detection intrusion systems. The second one, was detection of anamoly-based, comparing new set of data with a model of users normal behaviour and makes a significant deviation in this model. It is anomaly based and uses machine learning. And here, applying a deep learning approach or method to this solution helps for detecting anomaly in an any SDN environment. Hence building a Deep Neural Network (DNN) model for detecting such intrusion in the detection system and being trained, the above model with the NSLKDD Dataset. In this way, it has just used six basic features (that has been easily obtained in such SDN environment) that has been taken from the forty one such features of NSL-KDD Dataset. This system of anomaly detection uses deep learning. In this paper, it was found to apply a Deep Neural Network (DNN) and uses it for the NIDS model in an any context of SDN. They have trained and evaluated this model by using the NSL-KDD Dataset(a set of new data).Here, a deep learning algorithm was used for detecting intrusion in the network and evaluating NIDS model. Although these results are not yet good enough, they have yet to be adopted in any commercial product for approach on signature-based IDS, where still it has significant potential and certain advantages for further more development.To improve accuracy, it will analyze the network traffic and proposes the other types of features. With more flexibility in the model of the SDN structure, it can extract many features containing more valuable information or focusing on any one specific type of attack, like DDoS, hereby increasing accuracy of NIDS.

J. An Efficient DDoS TCP Flood Attack Detection and Prevention System in a Cloud Environment

AQEEL SAHI, DAVID LAI , YAN LI , (Member, IEEE), AND MOHAMMED DIYKH

Although it was found to be a number of cloud projects, it has dramatically increased over the last years, ensuring the availability and security of services, and resources is still found to be crucial and challenging issue. In this context,Distributed denial of service (DDoS) attacks were found to be the second most prevalent attacks of cybercrime following information theft. Here, DDoS TCP flood attacks are considered and it can exhaust the cloud's resources, consuming most of its network bandwidth, and damaging the entire cloud project within a shorter duration of time. This timely detection and preventing such attacks in cloud projects are found to be more vital, especially for eHealth clouds. In this paper, it has been presented that a new classifier system for detecting such attacks and prevents DDoS TCP flood attacks (CS_DDoS) in public clouds. Thus the proposed above CS_DDoS system was found to offer a solution to secure stored records by classifying them in incoming packets and thus makes a decision based on the obtained results. During the earlier phase of detection, the CS_DDOS identifies and determines whether a packet was found to be normal or originating from an attacker.And now during the phase of prevention, the packets, which were classified as malicious, will be denied to access such cloud services and the main source IP will be blacklisted shortly. Including the performance of the CS_DDoS system it was compared with the different classifiers or algorithm like least squares supporting vector machine (LS-SVM), naïve Bayes, K-nearest, and multilayer perceptron. Finally the results obtained will show that CS_DDoS yields best performance when the LS-SVM classifier is chosen. And it can also detect DDoS TCP flood attacks with about 96.7% accuracy and with a Kappa coefficient of 0.88 under attack from a single source, and 93.4% accuracy with a Kappa coefficient of 0.89 under attack from many attackers. Then the results were discussed in terms of accuracy and time complexity, and validating using a K-fold cross-validation model. Thus the proposed approach was found to efficiently improve the security of records, and to reduce the bandwidth consumption.

K. **Feature selection using the domain relationship with genetic algorithms**

N. Chaikla and Y. Qi

In this paper considering the importance of the relationship of domain, eliminating noisy features in feature selection was considered prior, and they have presented an alternate approach to design a multi-objective fitness function. This has been accomplished using multiple correlation for the genetic algorithm (GA), which has been used as a search tool in the above mentioned problem. Here using multiple correlation was a simple statistical technique that was found to be used coefficients of multiple correlations to measure or to identify the relationship between a dependent variable and a set of independent variables. This relationship is found within the domain space. Even simulation studies were been conducted in both real-world and controlled data sets to find the performance of the proposed methos or the fitness function. This comparison between the traditional approach or fitness function and the originally proposed function were also reported. Then the results show that the proposed fitness function can perform more function that is satisfactory than the traditional one in all cases. It also includes different data types, multi-class and multi-dimensional data. There have also been a large number of algorithms that have been proposed for feature subset selection. Some experimental results shows that the sequential forward floating selection (SFFS) algorithm is also a better approach that has been tested along with the other set of algorithms for feature selection method. The study of problem of choosing a feature set for the use of classification based on even SAR satellite images using different texture models. It was also found that pooling features deriving from other different texture models, also followed by a feature selection results in a substantial improvement in the accuracy of classification. It was also illustrated with the dangers of using feature selection in small sample situations.

L. **Trees vs neurons: Comparison between random forest and ANN for high-resolution prediction of building energy consumption.**

M. W. Ahmad, M. Mourshed, and Y. Rezgui

In the predictive analytics played in this paper, it was found that a significant role regarding to ensure an optimal and secure operation of power systems, along with reducing energy consumption and to detect the fault and thereby to diagnose and to improve the grid resilience. However, due to some nonlinearities in system there are some problem because of many influencing factors like climate, users' behaviour, their pattern and their building type was a challenging task to get accurate energy consumption prediction. This paper investigates more about the accuracy and to generalize the capabilities of deep highway networks (DHN) and use of extremely randomized trees (ET) used for predicting hourly heating, along with ventilation and air conditioning (HVAC). Their performance was also compared with the support vector regression (SVR), which is a most widely used supervised machine learning algorithm in recent time. Obtained results were found that both ET and DHN models marginally performs the above SVR algorithm. The paper also provides some details about the impact of increasing the deep highway network's complexity based on its performance. This paper concludes with all the developed models with equally applicable for predicting hourly HVAC energy consumption. Here the possible reasons for the minimum impact of such complexity and further research work were also highlighted in this paper.

M. Fuzzy sets in Fuzzy Sets, Fuzzy Logic, and Fuzzy Systems

L. A. Zadeh

Soft computing,here being opposed to traditional computing, deals with approximate models and thus giving solutions to more complex real-life problems. Here, unlike hard computing,a soft computing is more tolerant to imprecision, little uncertainty, a partial truth, and certain approximations. Prior to this effect, this role model for soft computing is generally equivalent to human mind. Generally a soft computing is based on techniques such as fuzzy logic, certain logical genetic algorithms, and artificial neural networks along with machine learning and expert systems. Although this soft computing theory and techniques were first introduced in 1985s, it was found to become a major research and study area in automatic control engineering. It was also found in this

paper or the approach that this technique of soft computing are nowadays being used successfully in recent many domestic, commercial, and industrial applications. And along with the advent of the low-cost and very high performance processors which are digital and the reduction of the cost of memory chips was also clear that the techniques and application areas of soft computing will continue to expand. Advently, this paper finally gives an overview of the current state of soft computing techniques and therefore describing the advantages and disadvantages of soft computing compared to other traditional hard computing techniques.

N. A Novel DoS and DDoS Attacks Detection Algorithm Using ARIMA Time Series Model and Chaotic System in Computer Networks

S. M. T. Nezhad, M. Nazari, and E. A. Gharavol

This paper deals with the matter of detective work DoS and DDoS attacks. 1st of all, twofeatures as well as range of packets and range of supply information processing addresses square measure extracted from network traffics as detection metrics in each minute. Hence, a statistic supported the number of packets is made and normalized employing a Box-Cox transformation. An ARIMA model is additionally used to predict the amount of packets in each following minute. Then, the chaotic behavior of prediction error statistic is examined by computing the most Lyapunov exponent. The native Lyapunov exponent is additionally calculated as an acceptable indicator for chaotic and nonchaotic errors. Finally, a collection of rules square measure projected supported repeatability of chaotic behavior and massive growth within the magnitude relation of range of packets to range of source information processing addresses throughout attack times to classify traditional and attack traffics from every other.This algorithmic program making an attempt to own quality in detection methodology. any network for that matter, is low in memory and power that the additional light-weight the answer the higher.Furthermore, the foremost false positives generated from this detection engine were below the slow-rate attack situations. above all, less options that square measure used with detective work the slow-rate attack. every network produces its own heterogeneous traffic therefore malicious behaviour goes to differ looking on the sort, size, and intensity of the attack and what the target is. Hence, cross-network attacks square measure a possible situation since such a large amount of networks are interconnected along and communicate with one another on a continuing and continuous way. it's not protected against external threats conjointly from internal threats that aim to abuse its normal functioning and force it to participate in large-scale DDoS attacks that aim to threaten the target crucial infrastructure.Whereas we have a tendency to square measure implementing a giant knowledge primarily based centralized log analysis system to spot the network traffic occurred by attackers through DDOS,addressing additional options SQL Injection and Bruce Force attack. we have a tendency to six completely different attacks that is formed by assailant. 1) Request from Id with additional range of your time from inside a time-frame, 2)Request from same Id with completely different inside short time, 3) Request from different Id ,same request from completely different information processing with multiple time, 4) Request from completely different Id,different request , completely different information processing during a multiple time, 5) SQL injection 6) Brute forceattack.The log file is mechanically transmitted to the centralized cloud server and massive knowledge is initiated for analysis method. This algorithmic program making an attempt to own terribly less quality in detection methodology. The no false positives generated from this detection engine. it's protected from external threats conjointly from internal threats that aim to abuse its traditional functioning and block them.

O. A DDoS Attack Detection Method Based on Hybrid Heterogeneous Multiclassifier Ensemble Learning

B. Jia, X. Huang, R. Liu, and Y. Ma

In this paper, they have got proposed a DDoS assault detection technique based on hybrid heterogeneous multi classifier ensemble mastering and design a heuristic detection algorithm based totally on Singular Value Decomposition (SVD) to construct our detection device. Through the comparisons with Random Forest, *k*-Nearest Neighbour (*k*-NN), and Bagging comprising the issue classifiers when the 3 algorithms are used alone through SVD and by un-SVD, it's far proven that this version is advanced to the brand new assault detection strategies in system generalization ability, detection stability, and basic detection performance .This system is fantastically time eating as it has to method the data classify them and then stumble

on the DDOS attack . Since they use classification algorithm the possibilities of false positives and actual negatives also are there .Also their process requires data pre-remedy due to the fact the training subset of 10 percentage and the "corrected" trying out subset in KDD CUP 1999 data set include masses of hundreds of network records, the hardware configuration of our sever can't load the calculation to method the abovementioned statistics sets. Here, they use the built-in "random ()" technique in MySQL to randomly select one in each ten information of the education subset and checking out subset as our information sets .But our paper doesn't involve any type of facts pre-remedy and classifiers to detect the DDOS attack as an alternative we simply use the less time ingesting divide and conquer technique to stumble on the attack .Also in our method we do now not have to use any schooling facts set foe classifying therefore no storage could be required for storing them too.

P. DDoS Detection System: Using a Set of Classification Algorithms Controlled by Fuzzy Logic System in Apache Spark

Amjad Alsirhani , Member, IEEE, Srinivas Sampalli , Member, IEEE, and Peter Bodorik, Member, IEEE

In this paper, they have proposed a dynamic DDoS attack detection system based on three main components: 1) classification algorithms; 2) a distributed system; and 3) a fuzzy logic system. Thier framework uses fuzzy logic to dynamically select an algorithm from a set of prepared classification algorithms that detect different DDoS patterns. Out of the many candidate classification algorithms, they use Naive Bayes, Decision Tree (Entropy), Decision Tree (Gini), and Random Forest as candidate algorithms. They have evaluated the performance of classification algorithms and their delays and validated the fuzzy logic system. They have also evaluated the effectiveness of the distributed system and its impact on the classification algorithms delay. The results show that there is a trade-off between the utilized classification algorithms' accuracies and their delays. They have observed that the fuzzy logic system can effectively select the right classification algorithm based on the traffic status. Currently, our system is designed to analyze static network traffic data. Our system is able of capturing and storing network traffic data in an HDFS database, waiting for batch processing. We will extend the proposed method to handle real streaming data from all sources. Thus, the DDoS attack can be detected in near real-time. 2) The iteration T time was statically set. However, in the future, we will investigate an effective and dynamic mechanism to update the iteration time. 3) The dataset was updated each iteration in case the traffic data is classified as a DDoS attack. However, currently, our system uses the same dataset with different sizes and different feature dimensions to simulate the update process. In the future, we will investigate the update process including data labelling as well as the increase of the dataset size. 4) Furthermore, we will investigate how to make deep learning an integral part of our detection process, at the same time maintaining low model training time. Whereas our paper is implemented using Big Data based centralized log analysis system .The analysis of the centralized log is done using divide and conquer algorithm .Thus providing improvements like IP address(zombie clients) will be blocked if DDOS attack is recognized .Check behaviour of user .Block unauthorized accessing of user through checking on SQL injection .Integrating big data in this project will help in dynamic analysis of real streaming data from all sources .Increase performance rate with decrease in computational overhead.

Q. Detecting Web based DDoS Attack using MapReduce operations in Cloud Computing Environment

Junho Choi, Chang Choi, Byeongkyu Ko, Dongjin Choi, and Pankoo Kim∗ Chosun University, Gwangju, Republic of Korea

This study proposes a way of integration between HTTP GET flooding among DDOS attacks and MapReduce process for a quick attack detection in cloud computing setting. This technique is feasible to confirm the supply of the target system for correct and reliable detection supported HTTP GET flooding. In experiments, the time interval for performance analysis compares a clog detection of attack options with the Snort detection. The planned technique is best than Snort detection technique in experiment results as a result of time interval of planned technique is shorter with increasing congestion. the foremost typical response technique of HTTP GET flooding is that the analysis of request worth supported packet checking.This technique focuses specifically on HTTP GET alone and conjointly this map cut back is feasible solely on cloud computing setting . Whereas our paper addresses numerous different kinds of DDOS attack too like SQL Injection and Bruce Force attack. we

tend to six completely different attacks that is created by wrongdoer. 1) Request from Id with a lot of variety of your time from among a time-frame, 2)Request from same Id with completely different among short time, 3) Request from completely different Id ,same request from completely different scientific discipline with multiple time, 4) Request from completely different Id ,different request , completely different scientific discipline in a very multiple time, 5) SQL injection 6) Brute force attack .Also our paper proposes a concept of police work DDOS attack in any setting and not specifically any setting . The performance of our plan exploitation divide and conquer methodology is very economical and straightforward in comparison with exploitation map cut back operations that is specific to cloud computing setting. the target of the project is to seek out the attacks and block user and their credentials exploitation huge information. scientific discipline address(zombie clients) are blocked if DDOS attack is recognized. Check behaviour of user . Block unauthorized accessing of user through checking on SQL injection .Integrating huge information during this project can facilitate in dynamic analysis of real streaming information from all sources .Increase performance rate with decrease in procedure overhead.

R. Feature selection for robust backscatter DDoS detection.

E. Balkanli, A. N. Zincir-Heywood, and M. I. Heywood

This paper analyzes the result of victimization totally different feature choice algorithms for sturdy break up DDoS detection. to realize this, we tend to analyzed four {different|totally totally different|completely different} coaching sets with four different feature sets. we tend to utilized 2 well-known feature choice algorithms, specifically Chi-Square and Symmetrical Uncertainty, along side the choice Tree classifier. All the datasets utilized square measure in public offered and provided by CAIDA. Our experimental results show that it's potential to develop a strong detection system which will generalize well to the dynamical break up DDoS behaviours over time employing a little variety of selected options .The quality of those algorithmic rules square measure terribly high compared to the divide and conquer algorithm that's utilized in our paper .Also the process of analysing the coaching knowledge sets and totally different feature knowledge sets square measure time intense too .They have used 2 algorithmic rules and a classifier whereas our paper needs the employment of only 1 algorithm and no classifiers one by one .And victimization their technology they will solely discover the presence or incidence of a DDOS attack whereas there's no technique to stop to pass though that attack .But our paper proposes a thought for not solely detective work the DDOS attack however conjointly to spot the individual scientific discipline from wherever the attack originated and block them from causing more DDOS request messages .Thus our plan helps in sick from the DDOS attack providing rather more economical resolution to discover and pass though totally different DDOS attacks. The analysis of the centralized log is finished victimization divide and conquer algorithmic rule .The six {different | totally, totally different| completely different} attacks that is created by attacker:1) Same request from different Id among a timeframe 2) totally different request from same Id among a timeframe 3) Multiple same request from one Id, within a timeframe 4) {different |totally totally different |completely different} request from different Id in a very multiple time 5) SQL injection 6) Brute force attack The log file is mechanically transmitted to the centralized cloud server and metallic element g knowledge is initiated for analysis method.

S. Efficient detection of DDoS attacks with important attributes.

W. Wang and S. Gombault

In this paper, they have used the chi-square and Information gain feature selection mechanisms for selecting the important attributes. With the selected attributes, various machine learning models, like Navies Bayes, C4.5, SVM, KNN, K-means and Fuzzy c-means clustering are developed for efficient detection of DDoS attacks. Then their experimental results show that Fuzzy c-means clustering gives better accuracy in identifying the attacks. Detection schemes involve complex computations due to which time taken by the system is too long to find the anomalous conditions. Therefore, detection speed must be given preference over detection accuracy for the disclosure of attacks in real-time. It should be effective against a variety of attack tools available today. Therefore, it should not be exposed to attacks, producing an impending disruption of its services. The detection procedures should rest on a small fraction of input (traffic) parameters, and sturdy against future trials by the attacker. It should be capable of handling the masses and functions accurately in high-speed real networks. The analysis of the centralized log is finished victimization divide and conquer algorithmic rule .The six {different | totally, totally different| completely different} attacks that is created by attacker:1) Same request from different

Id among a timeframe 2) totally different request from same Id among a timeframe 3) Multiple same request from one Id, within a timeframe 4) {different |totally totally different |completely different} request from different Id in a very multiple time 5) SQL injection 6) Brute force attack The log file is mechanically transmitted to the centralized cloud server and metallic element g knowledge is initiated for analysis method. IP address(zombie clients) will be blocked if DDOS attack is recognized.Check behavior of user.Block unauthorized accessing of user through checking on SQL injection.Integrating big data in this project will help in dynamic analysis of real streaming data from all sources.Increase performance rate with decrease in computational overhead.

III.PROPOSED WORK:

The proposed idea is that, an intelligent algorithm is employed at the zombie client itself which is capable of distinguishing between the legitimate and illegitimate requests from the client in which it is running.The six different attacks which is made by attacker:

1) Same request from different Id within a time frame

2) Different request from same Id within a time frame

3) Multiple same request from one Id, within a time frame

4) Different request from different Id in a multiple time

5) SQL injection

6) Brute force attack

After the classification of illegal requests from the legal ones the algorithm makes sure that those requests are never sent to the server.

IV.CONCLUSION:

Thus the project conclude that through this system we identify the zombie clients, their attacks and log file separately from the client side itself.

V.REFERENCES:

[1] S. M. T. Nezhad, M. Nazari, and E. A. Gharavol, “A novel DoS and DDoS attacks detection algorithm using ARIMA time series model and chaotic system in computer networks,” IEEE Commun. Lett., vol. 20,no. 4, pp. 700–703, Apr. 2016.

[2] B. Jia, X. Huang, R. Liu, and Y. Ma, “A DDoS attack detection method based on hybrid heterogeneous multiclassifier ensemble learning,” J.Elect. Comput. Eng., vol. 2017, no. 2, pp. 1–9, 2017.

[3] A. Alsirhani, S. Sampalli, and P. Bodorik, “DDoS attack detection system: Utilizing classification algorithms with Apache Spark,” in Proc. 9th IFIP Int. Conf. New Technol. Mobility Security (NTMS), Feb. 2018, pp. 1–7.

[4] J. Choi, C. Choi, B. Ko, D. Choi, and P. Kim, “Detecting Web based DDoS attack using mapreduce operations in cloud computing environ- ment,” J. Internet Services Inf. Security, vol. 3, nos. 3–4, pp. 28–37,2013. [Online].

[5] E. Balkanli, A. N. Zincir-Heywood, and M. I. Heywood, “Feature selection for robust backscatter DDoS detection,” in Proc. IEEE 40th Local Comput. Netw. Conf. Workshops (LCN Workshops), Oct. 2015,pp. 611–618.

[6] W. Wang and S. Gombault, "Efficient detection of DDoS attacks with important attributes," in Proc. 3rd Int. Conf. Risks Security Internet Syst., Oct. 2008, pp. 61–67.

[7] X. Yuan, C. Li, and X. Li, "Deepdefense: Identifying DDoS attack via deep learning," in Proc. IEEE Int. Conf. Smart Comput. (SMARTCOMP),2017, pp. 1–8.

[8] S. Hameed and U. Ali, "Efficacy of live DDoS detection with Hadoop," in Proc. IEEE/IFIP Netw. Oper. Manag. Symp. (NOMS), 2016, pp. 488–494.

[9] M. Mizukoshi and M. Munetomo, "Distributed denial of services attack protection system with genetic algorithms on Hadoop cluster comput-ing framework," in Proc. IEEE Congr. Evol. Comput. (CEC), 2015,pp. 1575–1580.

[10] H. Badis, G. Doyen, and R. Khatoun, "Understanding botclouds from a system perspective: A principal component analysis," in Proc.IEEE/IFIP NOMS IEEE/IFIP Netw. Oper. Manag. Symp. Manag. Softw.Defined World, 2014, pp. 1–9.

[11] C. Yin, Y. Zhu, J. Fei, and X. He, "A deep learning approach for intru-sion detection using recurrent neural networks," IEEE Access, vol. 5,pp. 21954–21961, 2017.

[12] P. J. Criscuolo. (2000). Distributed Denial of Service Tools Trinoo, Tribe Flood Network, Tribe Flood Network 2000, and Stacheldraht. [Online].Available: https://e-reports-ext.llnl.gov/pdf/237595.pdf

[13] R. Song and F. Liu, "Real-time anomaly traffic monitoring based on dynamic K-NN cumulative-distance abnormal detection algorithm," in Proc. 3rd Int. Conf. Cloud Comput. Intell. Syst., vol. 2, pp. 187–192,2014..

14] K. M. Prasad, A. R. M. Reddy, and K. V. Rao, "Discriminating DDoS attack traffic from flash crowds on Internet threat monitors (ITM) using entropy variations," Afr. J. Comput. ICT, vol. 6, no. 2, pp. 53–62, 2013.

[15] T. A. Tang, L. Mhamdi, D. McLernon, S. A. R. Zaidi, and M. Ghogho,"Deep learning approach for network intrusion detection in software defined networking," in Proc. Int. Conf. Wireless Netw. Mobile Commun.(WINCOM), Oct. 2016, pp. 258–263.

[16] A. Sahi, D. Lai, Y. Li, and M. Diykh, "An efficient DDoS TCP flood attack detection and prevention system in a cloud environment," IEEEAccess, vol. 5, pp. 6036–6048, 2017.

[17] N. Chaikla and Y. Qi, "Feature selection using the domain relationship with genetic algorithms," Knowl. Inf. Syst., vol. 1, no. 3, pp. 377–390,Aug. 1999. [Online].

[18] M. W. Ahmad, M. Mourshed, and Y. Rezgui, "Trees vs neurons:Comparison between random forest and ANN for high-resolution prediction of building energy consumption," Energy Build., vol. 147,pp. 77–89, Jul. 2017. [Online].

[19] L. A. Zadeh, "Fuzzy sets," in Fuzzy Sets, Fuzzy Logic, and Fuzzy Systems: Selected Papers by Lotfi A. Zadeh. Singapore: World Sci., 1996,pp. 394–432.