Comparative Analysis on DDoS DetectionTechniques

Akshat Shrivastava

Information Technology Delhi Technological University
Delhi, India akshshri2013@gmail.com

Kapil Sharma
Information Technology Delhi Technological University
Delhi, India kapil@ieee.org

***Abstract*—**Cyber security is always a topic of concern in the IT world. As the internet and types of devices, and domains in which these devices are used for sharing information are increasing also resulting in cyber threats to increase rapidly. Distributed Denial of Service (DDoS) attack is one of them which is quite simple to execute but it has the capability to shut down an entire country from several hours to days. Now in order to prevent the DDoS attack we need detection techniques, which can detect these attack at appropriate time so that mitigation steps can be taken accordingly. Many researchers have proposed different types of detection techniques. This paper focus on different types of DDoS detection techniques which are present for different types of devices which are connected in networks. The study will have a comparative analysis of available detection techniques on different parameters and also providing an overview of techniques. This paper will also discuss about performance of all the models and a comparative analysis of it. This article will conclude with discussion, analysis and recommendations in order to make DDoS detection techniques more reliable and better.

***Index Terms*—DDoS Attack, Cyber-Security, Internet of Things (IoT), Unmanned Aerial Vehicle (UAVs), Machine Learn-ing, Smart City**

I. INTRODUCTION

With the evolution of computers and the internet the task of human beings is becoming easier, but from the start they are becoming vulnerable for cyber attacks. IT security is nowadays becoming one of the important aspects as the demand for it is increasing continuously. There are many types of threats but Denial of Service (DoS) / Distributed Denial of Service (DDoS) are among ones which are quite simple to perform but in result they can cause severe loss in terms of resource utilization, bandwidth utilization and other internet resources. DDoS is the attack which is actually very difficult to recog- nize and follow up because it is very difficult to differentiate between DDoS attack packet and normal packet and also it is happening online so the window for identifying and taking steps for it is very limited[1].

According to the WWW FAQ[2] Distributed Denial of Service (DDoS) attacks can be defined as “A DDoS attack uses many computers to launch a coordinated DoS attack against one or

more targets. Using client/server technology, the perpetrator is able to multiply the effectiveness of the DoS significantly by harnessing the resources of multiple unwitting accomplice computers, which serve as attack platforms"[3].

DDoS attack is more dangerous form of DoS attack and its impact can vary from low to very high for different areas of internet applications. As with the growth of the internet for many different types of applications this attack is impacting the devices and its related resources in different ways. Also these different applications have their own limited types of resources so it is difficult to implement the same type of detection and mitigation technique for this attack. Various DDoS attack detection techniques have been developed and they all are using various types of concepts in order to fill the gaps of one or other methods, but different domains of network have there own advantage and disadvantage which can be used for detecting the attack. Following are some domains where DDoS attack is becoming dangerous day by day.

A. Internet of Things (IoT)

Internet of Things (IoT) are the physical gadgets and devices which make use of the internet in order to complete their tasks. These types of gadgets can now be found everywhere. The IoT is now becoming a very efficient medium for sharing informa- tion among people. IoT is basically a combination of devices, objects and sensors along with the internet for communication. The internet of things has vast applications involving from the daily household gadgets like light bulb, home theater etc.to agriculture products in order to increase productivity. It finds its application in military operations, health care systems etc. We can say an IoT ecosystem has been formed which is consisting of intelligence systems that are embedded with sensors, processors, devices which collect information using internet and use that information to complete their tasks So as these devices are making use of network of internet in order to collect information and use it these are becoming vulnerable to DDoS attack and various other intrusion attacks. And as these devices are continuously growing in numbers so this attack can cause good harm to devices but also to the public. But as IoT devices have limited computational resources, following conventional intrusion detection system is difficult[4]. Various detection techniques have been proposed for IoT devices in order to tackle the DDoS attack. The IDS are applied on the network and deep learning models have outperformed traditional machine learning models[5]. For Iot network the dataset can be big, so meta-heuristics algorithm

can be applied to work with these types of data[6][7]. And as these dataset are used for ML models so they can be applied with less computation.

B. Smart Cities

Nowadays the concept of smart cities is booming and every country is now moving towards the phase where smart city will be an important part of its country. Smart city can be said as a city which is having the implementation of Information Communication Technologies (ICT). These smart cities are meant to be built for improving the livelihood and make the city more reliable with an increase in population. These cities are composed of technology which

means they are incorporated with intelligent systems which are capable of sharing information and performing tasks using the internet. The representation of smart city can be seen in Fig. 1. As technology enters it gets vulnerable to different threats. And one of the important threats for smart cities is the cyber threat, which is the most common threat. These cyber threats can be of many forms, among them DDoS attack is also one of the dangerous attacks which can be part of it[8]. These smart cities involve a large amount of networking and getting invaded with DDoS attack can cause catastrophe in the city. It will not only lead to resource utilization but also can be dangerous for the common public. Although the detection method for DDoS can be implemented in smart city formulas, it is one of the challenges to get it right.

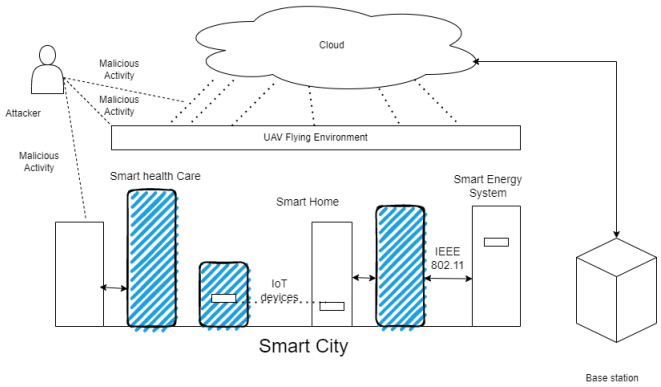

Fig. 1: Smart City Representation

C. *Cloud Technology*

Cloud computing can be termed as a large distributed computing paradigm. It can be termed as sharing of resources in an organized way so that every request can be deliverable. This technology is gaining popularity because of the advantage that the user does not need to buy the hardware or any infrastructure for it, instead it can use third party cloud services to fulfill its tasks. So these cloud services are basically provided through the internet making it one of the vulnerable targets for cyber attacks. DDoS attack can be a good tool to bring down the entire cloud service of any vendor to halt. So as the primary victim the attack of DDoS will be on the cloud but it will impact way more than that for all the users who are using these cloud services. So there is a need for an intrusion detection system which can read the pattern of the network and using different detection techniques it can identify the attack. There are many detection techniques which have been proposed like various machine learning models and also deep learning models.

D. *Unmanned Aerial Vehicle*

Nowadays drones are not only part of military operations but now it has started gaining its popularity in the commercial world. These drones are now part of various Multinational Companies which are used to complete their tasks and also these devices are getting used for agriculture, surveillance systems, weather monitoring systems, difficult areas where human reach is not possible etc. So basically these drones are having their own ecosystem as the

Internet of Drones (IoD) [9]. The representation of IoD can be seen in Fig. 2 As the communication between the drones and user at ground level is mostly with wireless networks making it a very good option for intrusion attacks. DDoS attack can be very dangerous for drones as if the drones are not only a single drone if it involves more than one drone then it will result in complete utilization of network bandwidth and which will lead to getting no signal from the controller so it can even harm the public if it gets crashed. In order to tackle this attack various methods for detection have been proposed involving blockchain to machine learning models to deep learning.

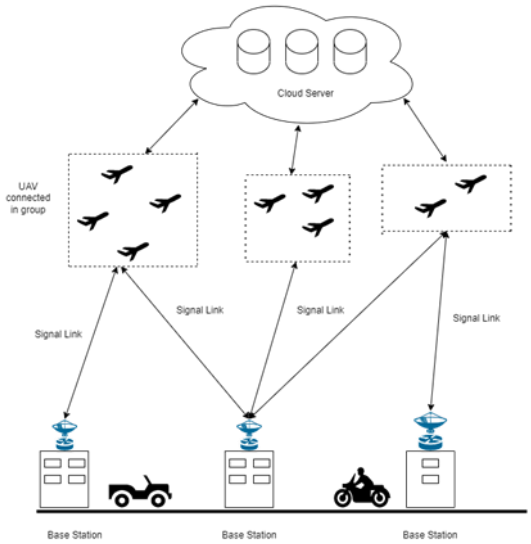

Fig. 2: IoD Representation

E. Common Networks

Computer technology is now becoming part of every sector in the whole world. Each sector whether it is government, private, public, educational, agriculture, military, health care etc. all things are nowadays revolving around technology. And the internet is one of the important threads which play a vital role in making it all possible. So as the internet is involved it means it is prone to various cyber attacks. DDoS attack is one of them which occurs as it is simple to implement and it has capability of halting the entire country's system if attacked in a dangerous manner. DDoS attacks can be targeted to any server whether its of any company or any institution. Although it makes use of all the resources it can make an impact on all other users which are using that service. There are many models and techniques which have continuously been invented in order to detect the DDoS attack and in very short time it can be put to halt. Different machine learning models, deep learning models, different statistical techniques etc. have been proposed in order to detect the DDoS attack. Also different soft computing concepts involving efficient classifier for detection and prevention are being developed and as there performance is good they are applicable for different intrusion detection attack[10].

In this paper different types of DDoS detection techniques which are targeting different domains of networks have been studied. In section II, DoS/DDoS attack has been explained. In Section III, Various types of DDoS detection techniques have been studied then in section

IV, Discussion of these techniqueshas been done in Section V, Analysis these techniques have been presented along with some recommendations and sectionVI will bring the conclusion to work.

II. DENIAL OF SERVICE (DOS) / DISTRIBUTED DENIAL OF SERVICE (DDOS) ATTACK

DoS attack or Denial of Service attack is an attempt byan attacker such that it hampers the normal user service ofany network or any other internet application. This attackcannot cause corruption in data but its main target is to block the resources of any server or any application. DoS attacks normally attack on a network causing entire usage of band- width which result in large amounts of traffic on the network such that it causes complete utilization of operating system resources of server or any application making it difficult to access the system by any normal user. The victim of this attackcan be a single router or can be the entire network of any organization. The attacker will supply such a huge number of baseless packets so that it can make a service unavailable fora few hours to a few days. In the similar manner Distributed Denial of Service (DDoS) attack is a more dangerous formof DoS attack. This attack becomes more powerful by its property of distributing over the internet and causing massive traffic on the network. This attack takes advantage of open internet architecture. Due to its open design it becomes more vulnerable for DDoS attack. It can be understood by two reasons 1. Every internet host is occupied by limited resources which can serve only a limited number of users but this attack takes all the resources in its use. 2. Even though wecan make our system protected, it will always depend on the global internet. Therefore becoming vulnerable to attack. DDoS attack process can be understand using following Fig. 3 and steps:

- Attackers are one which is responsible for attack and he is the one who will do all preparations for attack.

- Then the attacker communicates with handlers through TCP,UDP or ICMP such that these handlers will be responsible to communicate with agents under them and when the attacker communicates to the handler about the attack then these handlers communicate this information to agents for attack.

- Then, when handlers order the agents which are having the code which will be responsible for the attack, agents get active and they start flooding the victim's machine.

And in this way when there are thousands or more agents at same time attacking the target machine it will cause a slowdown of the machine or complete shutdown of the system. And hence DDoS attacks become successful.

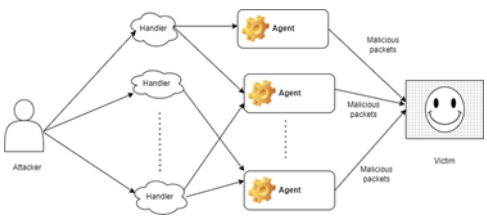

Fig. 3: Overview of DDoS Attack process

III. DDOS DETECTION TECHNIQUES

For any cyber attacks if we are having a proper detection technique then that attack can be identified at an early stage and it can be mitigated using appropriate methods. In this section we will be discussing different DDoS attack detection techniques on the basis of several parameters and we have summarized all these methods in table I.

In [11] they have used wavelet analysis for getting temporal correlation for various time scales. And in this method they have mentioned that it will require minimum computation for detection. Also they have used the Energy prediction model on wavelet analysis for detecting the DDoS attack in the network. According to this model during the normal circumstances when there is regular flow of data packets over internet there will be almost constant flow i.e. the projection which we will see in graph will not vary daily there can be some variation although, So when we see it using energy prediction model it will show slight variation in graph but when there is attack then there will be sudden and more variation in graph such that it can be identified as there is some attack on system. There will be spikes in the graph during the attack in the graph. So if these spikes in energy prediction models are captured in early stages of attack then this attack can be identified and it can be stopped in early stages.

In [1] the author has used a method for detecting the attack using a covariance model for detecting SYN flooding DDoS attack. The researcher of this method claims that as comparison to other statistical methods their methods give more accurate results and in less computation time. The method which the researchers have proposed is also based on statistical analysis but it does not require pre-assumed packet distribution data. They have focused on three main points, first they claim to propose a more generalized correlation method to detect DDoS attack. They are using raw data of packets i.e. different flag fields which will be acting as different features for predicting the model. Second they tried to focus on features selection which will be used to predict the model. Third, this method of detection works online and it not only predicts the attack on heavy flood of packets but also it predicts attack on less amount of flooded packets. As this model claims to give a good amount of accuracy for predicting attack it makes it a very suitable model by using multivariate correlation analysis.

With the growing Internet of things devices in the world as it is making life all easier at the same time it is producing more vulnerability for DDoS attack. But for IoT devices there are many advantages in capturing the attack since IoT devices do not use a large number of servers as other devices use rather it uses limited resources and IoT devices generally perform tasks which are generally repetitive in nature making the traffic pattern repetitive in nature so it becomes an advantage for identifying the changes in traffic. So using these principles in

[12] the researchers have tried to use machine learning for detecting the DDoS attack. They use protocol, packet length etc. as features for predicting models. They have used many machine learning classifier models like random forest, support vector machine, decision tree and neural networks. They have created a pipeline which works on routers or firewalls to

identify the traffic changes in IoT devices network and alsothe identifying the device which can be a potential attacking asset. They have also done a good analysis on feature selection such that the hypothesis which they have taken that IoT traffic differs from nonIoT device traffic can be proved and with the help of this analysis the classifiers have given good accuracy for each model. And as the number of features are less so it has become computationally feasible such that it will become an efficient option for applying it to the real world.

In[13] this method of detecting DDoS attack is based on statistical mechanism called as continuous ranked probability score (CRPS) and exponentially smoothing scheme for better detection of DDoS attack. There are several statistical methods and also other methods developed before for detection of DDoS attack like a rank correlation method for DRDoS attack but it is based on the fact that reflectors when tend go close to victim it is linearly auto correlated. In Kullback-Leibler information distance is proposed to identify the attack but there is a problem of getting control over various ISP routers and in doing so we need to get support from them. Other model like general entropy and information distance model is used but the problem with this type of model is it requires normal traffic and manual detection of threshold is required and many others so these all types of methods require some assumption like most of the methods assumes that distribution of traffic is behaving like Gaussian curve. Another limitation is that they need manual detection of thresholds and also this threshold is not that properly used. So to overcome these limitations this method claims to give good results on the basis of continuous ranked probability score (CRPS) statistical metrics and exponential smoothing (ES) scheme for detection of attack. This CRPS is used basically to detect the DDoS attack as it will give variation between current readings and distribution of normal traffic. The Exponential smoothing (ES) is used to get small data packet rate attacks as it will make use of all measurements i.e. of current as well as previous. In this method no normalizing method is used. And the threshold is not manually calculated, rather it is automatic and ES is used in CRPS for observing the threshold of different attacks. And this method is a network free method so it can be applied to any type of network.

In [14] they have taken mean packet arrival time and applied it on fuzzy estimators so that attack can be detected. Basically when a normal internet source is used in the internet then it communicates through packet and each packet has fixed inter arrival time so if we take its mean which we call as historical mean as we will be comparing this mean with real time observed value during the attack. So if observed interval time is below the mean then we can say it is a sign off attack and if it is above or near to mean then it is normal traffic. Also this mean value can be applied to poisson distribution which these researchers have taken for estimation. A fuzzy estimator is like triangle shaped in which mean is between such that it is getting divided into two parts i.e. left side and other one is right side. If an observed value is present on the left hand side then it is malicious packet i.e. an attack has happened and if it is on right side then it is normal traffic.

In [15] the paper proposes a method in order to detect the DDoS attack using machine learning models for IoT bots. In this work they have worked on small data sets as well as large datasets and in both cases it is showing promising results. In this detection scheme they

have used Support Vector Machine (SVM) and K- Nearest Neighbor machine learning model in order to classify the packets into two i.e. normal packets and abnormal packets. They have performed an experiment in which they have made DDoS attacks on IoT devices and collected the data for various time intervals. Then they have preprocessed the data and applied the machine learning models on it. They have used the XOIC tool for experimentation for attacking and for capturing they have used Wireshark Tool to sniff the packets. Also in order to increase the accuracy of the models they have selected a packet information field and also to reduce computation space. Both algorithms are giving the accuracy of 0.9 and more.

In [16] the author has proposed a DDoS attack detection technique using clustering and entropy based methods in order to identify the malicious packets in the network. This method makes use of a fog layer for detecting the attack. Fog computing is a type of distributed computing in which storage devices and routers are introduced as layers in between IoT devices and cloud servers. Here in this method they are using the IoT devices which are connected to clouds and in between them there are fog nodes present. When data is collected by an Iot device it is sent to a fog node where it is processed then this processed data is sent to the cloud so data is passing through the fog nodes. So if the attacker attacks the IoT devices then according to the author's algorithm which is implemented at fog node it will detect the malicious packet and it will be discarding it. The algorithm is such that the fog node discards the packets on the basis of IP address. They have implemented this model on Omnet++ simulator and the results of the models are quite good. According to their results and all the evaluation parameters this method is giving good results for detecting the attack.

Cloud computing is trending nowadays because of its scalability and usability. Also the virtual machines are quite economical as compared to physical machines making cloud a good tool for performing complex computations. The attacker can launch a DDoS attack using the virtual machine making it even harder to detect the attacker. These attackers rent these virtual machines and make them used for tracking the cloud servers. In [17] the author has proposed the machine learning methods for detecting the DDoS attack on cloud at source side. The detection methods can be applied at the victim and source side according to the algorithm. In this paper machine learning is using the statistical features for different attacks and mitigating the attack. They have performed this detection system on four types of attack namely TCP-SYN attack, DNS reflection attack, SSH Brute force attack and ICMP flood attack. They have created a machine learning engine which takes all the statistical parameters from packets of each type of attack and then processes these packets in the engine if it predicts that data packet is malicious it discards it otherwise accepts it. In this they have performed different types of machine learning models namely Linear Regression, SVM, Decision tree, Naive Bayes, Random Forest , Gaussian mixture model for Expectation-Maximization, K- means. These models are showing good accuracy for more than 99% making it a suitable candidate for detecting the DDoS attack on cloud.

In [18] the author has detected the DDoS attack using the Radial basis function neural network (RBF-NN) and in order to optimize it Bat algorithm is being used. As machine learning methods which are statistically based are quite researched and have been applied, the methods using neural networks are very less researched but these are also good approaches

to detect the attack. This model has good accuracy making it viable for application in the cloud to detect DDoS attack.

As compared to traditional networking, Software defined networking is becoming more popular nowadays. Due to its programmable, dynamic architecture and flexibility it is getting adopted more frequently. But as it is part of the network only it is vulnerable for DDoS attack. The control plane which is used to manage the transmission and as this control plane is exposed making it a vulnerable target for DDoS attack. Decreasing DDoS attack is more challenging then old traditional network because Openflow switches can operate through flow entry from controller side. In [19] the author has used machine learning models in order to detect the DDoS attack. They have carried out these machine learning models on open sourced dataset which are containing dataset for ICMP, UDP and TCP flood attacks. And after measuring the accuracies of ML models they have applied different feature selection algorithms in order to compare their result with previous and also to reduce computational complexity by reducing features. The classifiers used in this approach are SVM, K-NN, ANN and Naive Bayes. And all the models show accuracy above 80% which is a good sign for using machine learning models for detecting DDoS attack in software defined networks.

Drones are evolving day by day and for their communication the internet is required making them good options for various types of intrusion detection. In [20] the author has defined a machine learning model for intrusion attacks consisting of DDoS attack as well. It is designed for 5G software defined security systems for UAV communication. The various machine learning models show promising results for it. Almost all of the models show good accuracy above 90%.

In [21] the author has proposed an experience based deep learning algorithm in order to improve Intrusion detection system which is applied in the UAVs network. They have experimented their algorithm in a simulation environment using MATLAB. In this system they have also implemented that if a malicious packet comes then also this algorithm is capable of making the decision of either to keep it or remove it.

When we are building any model for the real world in order to make it through and validate we need to test it and use some of the parameters in order to evaluate it. All these models have been tested and been performed either on simulator or on real world scenarios. Thus evaluation is important for these models. The evaluation parameters can be many and each model can have different evaluation schemes according to the model. The evaluation parameters can also be defined with the help of graphs. While some models like machine learning models shows there validation through defined parameters like Precision, Recall, Accuracy, F1-Score, ROC Curve, Correlation Coefficient, True Positive Rate, False Positive Rate, True Negative Rate, False Negative Rate, Confusion Matrix and many. The table II shows detailed comparisons of all detection schemes on different performance parameters.

IV. DISCUSSION

Our research study is about various types of DDoS detection techniques. We have analyzed these detection techniques from different domains. The table I represents the summary of

detection techniques which are based on different parameters. These are:

- Types of DDoS attack carried out by techniques
- The victim which is used for the detecting techniques
- Brief description of the method
- Advantages of methods
- Limitations of methods

There are seven detection methods which are using artificial intelligence for detecting the attack and five are using other methods giving us the hint that artificial intelligence is dominating technology and very successful in internet security and

TABLE I: Comparison of DDoS Detection Techniques on various parameters

Paper	Year Of Publication	Detection method	Target for type of DDoS attack	Victim	Description	Advantage	Limitation
[21]	2021	Experience Deep Learning Algorithm	Ping of Death, DoS, DDoS generic	Drones	This model uses experienced based deep learning algorithm for Intrusion detection system used for UAV networking environment.	• This algorithm is used to improve the working of Intrusion detection systems. • Also abnormal queues of malicious packets will be removed	It is tested on simulation but practical implementation can have slight variation
[16]	2021	Fog Computing and Entropy	Not specified	Internet of Things (IoT)	This model uses a fog node which is present in	• It can detect an attack at an early stage.	It can be applied only to IoT devices connected to

		variations		devices	between IoT devices and cloud to detect DDoS attack using entropy variations.	• Independent of routing protocol. • Independent of any type of transmitted packet. • Traffic overhead is low in the proposed model. • Attack detection time is less. • Does Not depend on previous data so it can detect new types of attack.	the cloud as the algorithm is being tested on fog nodes.
[20]	2021	Machine learning based Intrusion detection system	Generic DDoS attack along with other attacks	Drones	Machine learning models are used for detecting intrusion for drones in cellular connections.	• Model is designed for 5G technology based which can be used in future. • All types of attacks	Not found

						have been detected with good accuracy.	

TABLE I: Comparison of DDoS Detection Techniques on various parameters

Paper	Year Of Publication	Detection method	Target for type of DDoS attack	Victim	Description	Advantage	Limitation
[19]	2020	Machine Learning based models	ICMP flood attack, UDP flood attack TCP flood attack	Software Defined Networks	In this approach machine learning models are used and in order to reduce features different feature selection algorithms have been applied.	- These ML models can be put in SDN so that these models can auto-matically learn and can take necessary actions. - Computationally feasible as a feature selection algorithm will be applied.	Not found
[13]	2020	Measurement based statistical mechanism	SYN flood Smurf attack	Network	This model uses concept of continuous ranked probability score (CRPS) for detection of DDoS attack.	- Model is tested on several datasets giving better results. - This method uses a statistical mechanism which is quite efficient.	Not Found

[12]	2018	Machine Learning DDoS detection	HTTP GET flood, TCP SYN flood, UDP flood	Internet of Things (IoT) devices	In this model ML models and deep learning models are used for detecting DoS attack.	- Computationally feasible as less features are used. - All classifiers have accuracy higher than 0.99. - Can be used for real time detection.	This method is experimented on only IoT devices data.
[15]	2018	Machine learning based	HTTP, TCP and ICMP flooding	Internet of Things (IoT) devices	Machine learning model is used to predict the normal packets and abnormal packets.	It can work with small and large	Method predicts the attack on the basis of previous knowledge of the dataset so change in attack pattern can be difficult to predict.
[17]	2017	Machine Learning models	ICMP flooding attack, SSH Brute force attack, TCP-SYN attack, DNS reflection attack	Cloud	In this machine learning models are used for detecting four types of attack and mitigating the attack by removing the virtual machine which is predicted for attacking.	Tested on a real cloud environment and getting 99% accuracy.	Depending on previous data if a new type of attack arises it will be difficult to detect.

TABLE I: Comparison of DDoS Detection Techniques on various parameters

Paper	Year Of Publication	Detection method	Target for type of DDoS attack	Victim	Description	Advantage	Limitation
[18]	2017	Radial basis function neural network	HTTP flooding, UDP folding and Smurf attack	Cloud	In this model DDoS attack is detected using RBF-NN and it	Any RBF network optimized using the Bat algorithm can be	Computational complexity can be a disadvantage.

		(RBF-NN) using Bat algorithm			has been optimized using Bat algorithm to get better accuracies.	used for detecting attacks.	
[14]	2012	Fuzzy Estimator	H TTP Flood Attack	Network	Fuzzy Estimators are used to detect the DDoS attack.	It can identify the source from where the attack is originating	Method can give incorrect result for spoofed IPs.
[1]	2004	Co variance Model	SYN Flooding	Network	This method uses generalized correlation methods which are using different flags of data packets and feature selection for detecting DDoS attack.	• It does not require pre assumed packet distribution data. • T his method works online. • T his method can also predict attacks on low flooded data packets.	• All 6 flags are necessary to be used for this method. • .Hig h pocket rate is not included in the method.

							• Optimal observed time interval is not shown with any proof.
[11]	2003	Wavelet Analysis	UDP Flooding	Network	Energy prediction model is used for detection of attack by comparing spikes in resultant graph	• Attack can be identified in early stages • Less Com-putation is required.	• This method requires larger trace size as it needs sampling window as power • Boundary values for wavelet analysis are difficult to decide. • This method does not detect attack when the number of packets are less flooded.

TABLE II: Comparison of DDoS Detection Techniques on testing and resulting parameters

Paper	Year	Model tested by	Evaluation parameters	Accuracy/Efficiency of model
[20]	2021	Open source dataset is used	Confusion Matrix, Precision, Recall, F1 Score, False Negative rate, ROC curve analysis	Decision Tree has maximum accuracy of 99.99% and Gaussian and Naive Bayes have lowest
[21]	2021	MATLAB and NS2 simulator	Throughput	Data from graphs shows detection is successful
[16]	2021	Omnet++ simulator is used	Precision, Throughput, Packet Delivery Ratio and True Negative Rate (TNR)	Data from graphs shows detection is successful.
[13]	2020	Open sourced dataset is used	True Positive rate (TPR) and false positive rate (FPR) and false negative rate (FNR) are calculated	The method shows accuracy of 99%
[19]	2020	Exper imental setup is used in order to collect the data	Accuracy, Sensitivity, Specificity, Precision, F1-Score, ROC curve is also used	All machine learning models shows accuracy above 90%
[12]	2018	Experimental setup of various IoT devices and attacking device and victim to acquire dataset	Precision, Recall and F1-score of machine learning models are used	All ML models are showing above 99%
[15]	2018	xperimental setup to collect the dataset	Accuracy of models are used	• 95% accuracy for SVM model and 90% accuracy for KNN model for large feature set.

				• 97% accuracy for SVM model and 98% accuracy for KNN model for small feature set. • This method does not detect attack when the number of packets are less flooded.
[17]	2017	Real cloud settings are used for implementing model	Precision and F1 Score	All ML model shows accuracy over 93% and Random forest is highest accuracy with 94.96%.
[18]	2017	Open sourced dataset is used	lassifier accuracy and False positive rate	Bat - Radial basis function (BAT-RBF), Radial basis function (RBF) and Genetic Algorithm - Radial basis function (GA-RBF) shows accuracy of more than 98%
[14]	2012	Open sourced dataset is used	Correlation Coefficient is used	100% success rate
[1]	2004	Simulator	Sensitivity of Covariance Matrix Distance Method	100% successful
[11]	2003	NS Simulator	Deviation of energy distribution for normal and attacked traffic.	Data from graphs shows detection is successful.

these methods belong to different domains so giving us one more hint that they are adaptable to different conditions with less complexity.

In table II we have presented the summary of implementa- tion and results of all the detection techniques. The result of each detection technique is calculated on different parameters. Among all these methods four methods use simulators to test their methods and four methods have used open sourced dataset and four methods have performed experiments in order to collect dataset and test their methods. All the machine learning models are showing good accuracy and these models can be used as a pipeline and can be used online to detect the attack. The machine learning models uses more evaluation parameters then other methods making them more provenmethods for detection.The open source dataset which has been used in different techniques are DARPA99s dataset ,

LLS DDOS 1.0 DARPA dataset, NSL-KDD dataset and CSECIC-IDS2018.

V. ANALYSIS

On the basis of literature review for DDoS detection tech- niques this section presents analysis and some recommenda- tions. Following are points:

- We have discussed many domains of the network like IoT network, Cloud network, UAV network etc. which are vulnerable to the DDoS attack. And these all domains have different properties but attack is of the same type. The method should be scalable in such a way that it can be applied for different types of networks.

- Since DDoS attack is not one which starts immediatelyas soon as it is triggered, there are phases of low rate DDoS attack and high rate DDoS attack. But there are

some methods which are capable of either working on low rate DDoS attack or high rate DDoS attack. So these methods can fail in some scenarios where both rates of DDoS attack are necessary.

- Machine Learning is an emerging and a very powerful technique for identifying the attack in real time. But the problem with these machine learning models is they required previous data in order to predict the attack. Butif the attack pattern gets new which has not been trained by the model can cause it to fail as it will not be able to identify the new type pattern of attack.

- We know that testing every type of detection technique in the real world is quite difficult so they are tested on simulators. Since the real world is full of surprises and applying these detection techniques which are tested on a simulator can vary in result when applied in thereal world. So all factors for the real world must beconsidered.

- There are many types of other DDoS attacks which can also be tested by detection techniques and their resultscan also be discussed.

- These detection techniques are separate for each network so this is kind of overhead for the system. So the detection techniques must be crafted in such a way that they bear less overhead on the applied system.

- As every method has advantages and disadvantages soin order to cover each model's

weakness, hybrid models can also be proposed but keeping all the parameters in considerations and getting better results.

VI. CONCLUSION

DDoS attacks are becoming a big concern in the IT world. Even big giant IT companies are facing this issue. Due to this attack there is great loss in terms of resources, financial and other aspects to companies. The detection of this attack is becoming a hot topic among researchers but every technique has its own flaw and the attacker tries to use these flaws in order to attack. In this paper we have compared different types of detection techniques which correspond to different domains. As each domain has its own resources, these techniques are studied and presented as comparative ways to get good insights of it. In our study we have presented different aspects of the detection techniques in a way they can be studied and applied accordingly.

REFERENCES

[1] Jin, Shuyuan, and Daniel S. Yeung. ”A covariance analysis model for DDoS attack detection.” In 2004 IEEE International Conference on Communications (IEEE Cat. No. 04CH37577), vol. 4, pp. 1882-1886. IEEE, 2004.

[2] Stein, L. D. ”The World Wide Web Security FAQ, version 3.1. 2.” http://www. w3. org/Security/Faq/ (2002).

[3] Specht, Stephen, and Ruby Lee. ”Taxonomies of distributed denial of service networks, attacks, tools and countermeasures.” CEL2003-03, Princeton University, Princeton, NJ, USA (2003).

[4] Chauhan, Anamika, Rajyavardhan Singh, and Pratyush Jain. ”A Liter- ature Review: Intrusion Detection Systems in Internet of Things.” In Journal of Physics: Conference Series, vol. 1518, no. 1, p. 012040. IOP Publishing, 2020.

[5] Kishore, Raj, and Anamika Chauhan. ”Evaluation of deep neural net- works for advanced intrusion detection systems.” In 2020 4th Inter- national Conference on Electronics, Communication and Aerospace Technology (ICECA), pp. 1-8. IEEE, 2020.

[6] Tripathi, Ashish Kumar, Kapil Sharma, Manju Bala, Akshi Kumar, Varun G. Menon, and Ali Kashif Bashir. ”A parallel military-dog- based algorithm for clustering big data in cognitive industrial internet of things.” IEEE Transactions on Industrial Informatics 17, no. 3 (2020): 2134-2142.

[7] Tripathi, Ashish Kumar, Kapil Sharma, and Manju Bala. ”A novel clustering method using enhanced grey wolf optimizer and mapreduce.” Big data research 14 (2018): 93-100.

[8] Hamid, Bushra, N. Z. Jhanjhi, Mamoona Humayun, Azeem Khan, and Ahmed Alsayat. ”Cyber security issues and challenges for smart cities: A survey.” In 2019 13th International Conference on Mathematics, Actuarial Science, Computer Science and Statistics (MACS), pp. 1-7. IEEE, 2019.

[9] Yahuza, Muktar, Mohd Yamani Idna Idris, Ismail Bin Ahmedy, Ain- uddin Wahid Abdul Wahab, Tarak Nandy, Noorzaily Mohamed Noor, and Abubakar Bala. ”Internet of drones security and privacy issues: Taxonomy and open challenges.” IEEE Access 9 (2021): 57243-57270.

[10] Chauhan, Anamika, and Kapil Sharma. ”Intrusion detection systems: A Comparison of soft computing techniques.” In Journal of Physics: Conference Series, vol. 1478, no. 1, p. 012013. IOP Publishing, 2020.

[11] Li, Lan, and Gyungho Lee. ”DDoS attack detection and wavelets.” Telecommunication Systems 28, no. 3 (2005): 435-451.

[12] Doshi, Rohan, Noah Apthorpe, and Nick Feamster. ”Machine learning ddos detection for consumer internet of things devices.” In 2018 IEEE Security and Privacy Workshops (SPW), pp. 29-35. IEEE, 2018.

[13] Bouyeddou, Benamar, Benamar Kadri, Fouzi Harrou, and Ying Sun. ”DDOS-attacks detection using an efficient measurement-based statisti- cal mechanism.” Engineering Science and Technology, an international Journal 23, no. 4 (2020): 870-878.

[14] Shiaeles, Stavros N., Vasilios Katos, Alexandros S. Karakos, and BasilK. Papadopoulos. ”Real time DDoS

detection using fuzzy estimators." computers & security 31, no. 6 (2012): 782-790.

[15] Gurulakshmi, K., and A. Nesarani. "Analysis of IoT bots against DDOS attack using machine learning algorithm." In 2018 2nd International conference on trends in electronics and informatics (ICOEI), pp. 1052-1057. IEEE, 2018.

[16] Gaurav, Akshat, Brij B. Gupta, Ching-Hsien Hsu, Shingo Yamaguchi, and Kwok Tai Chui. "Fog layer-based ddos attack detection approach for internet-of-things (iots) devices." In 2021 IEEE International Conference on Consumer Electronics (ICCE), pp. 1-5. IEEE, 2021.

[17] He, Zecheng, Tianwei Zhang, and Ruby B. Lee. "Machine learning based DDoS attack detection from source side in cloud." In 2017 IEEE 4th International Conference on Cyber Security and Cloud Computing (CSCloud), pp. 114-120. IEEE, 2017.

[18] Velliangiri, S., and J. Premalatha. "Intrusion detection of distributed denial of service attack in cloud." Cluster Computing 22, no. 5 (2019): 10615-10623.

[19] Polat, Huseyin, Onur Polat, and Aydin Cetin. "Detecting DDoS attacks in software-defined networks through feature selection methods and machine learning models." Sustainability 12, no. 3 (2020): 1035.

[20] Shrestha, Rakesh, Atefeh Omidkar, Sajjad Ahmadi Roudi, Robert Abbas, and Shiho Kim. "Machine-learning-enabled intrusion detection system for cellular connected UAV networks." Electronics 10, no. 13 (2021): 1549.

[21] Khan, Inam Ullah, Arsin Abdollahi, Muhammad Asghar Khan, Irfan Uddin, and Insaf Ullah. "Securing Against DoS/DDoS Attacks in Inter- net of Flying Things using Experience-based Deep Learning Algorithm."(2021).