PERFORMANCE EVALUATION OF VARIOUS LERNER ALGORITHMS ON DISTRIBUTED DENIAL OF SERVICE (DDoS) ATTACKS

Vimal Kumar Parganiha[1], Shruti Gorasia[2], Rida Anwar[3]

[1]*Professor, Computer Science Department, Dimat, Chhattisgarh, India*
[2]*Research Scholars, Computer Science Department, Dimat, Chhattisgarh, India*
[3] *Research Scholars, Computer Science Department, Dimat, Chhattisgarh, India*

Abstract

Distributed Denial of Service (DDoS) is that the act of performing arts associates degree attack that prevents the system from providing services to legitimate users. It takes several forms, and utilizes several attack vectors. When productive, the targeted host might stop providing any service, give restricted services solely or give services to some users solely. Application band DDoS advance is gotten from the lower layers. Application band based DDoS attacks use honest to advantage HTTP asks for afterwards foundation of TCP three way duke afraid and overpowers the blow assets, for example, attachments, CPU, memory, circle, database manual capacity. Normal contour is formed from user's admission behavior attributes that is that the final assay to differentiate DDoS attacks from beam crowd. An aberration apprehension apparatus is planned in this cardboard to apprehension DDoS attacks application altered classifiers. Attacked as well as non-attacked data is being collected form the server for comparison, in which reduction is being performed through JAYA algorithm to minimize the data through which attacked data is being easily identified and is being secure. Application band DDoS advance are classified with the accurateness of 99.5% with Bagged Tree Ensemble Classifier (BTEC).

Keywords: *DDoS, JAYA Algorithm, Anomaly Detection, Application Layer, Classifiers, ICMP, TCP.*

----------***----------

1. INTRODUCTION

Computer Security in the principle includes privacy trustworthiness and handiness. The key dangers in security research territory unit rupture of privacy, disappointment of validity what are more, unapproved DoS. DDoS advance has acquired astringent accident to servers and can could cause even beyond browbeating to the development of latest web services. In Application band DDoS attacks zombies attacks the blow web servers by HTTP GET asks for (e.g., HTTP Flooding) and affairs all-embracing account annal from the blow server in cutting numbers. In addition example, antagonist runs a aberrant amount of questions through the casualty's internet searcher or database catechism to accompany the server down. Then again, another extraordinary marvel of system movement called streak swarm has been seen by analysts amid the previous quite a long while. On the web, "streak swarm" alludes to the circumstance when a substantial number of clients all the while access a mainstream site, which delivers a billow in movement to the website and may be able to cause the website to be for all intents and purposes inaccessible.

Web applicant conduct is mostly impacted by the anatomy of website and the way audience admission website pages. Application band DDoS attacks are advised as abnormality analytic conduct and accustomed for web admission conduct is activated to advance the archetypal contour which is activated for amid attacks movement from accustomed activity. The perusing conduct of a web applicant is articular with the anatomy of a site, which involves a colossal amount of web archives, hyperlinks, and the way the applicant gets to the Website pages. A accustomed website page contains assorted access to added built-in articles, which are alluded to as in-line objects. A website can be portrayed by the hyperlinks a part of the website pages and the abundance of in-line altar in every page. At the point if audience bang a hyperlink advertence a page, the affairs will back assorted solicitations for the page what's more, its few in-line objects.

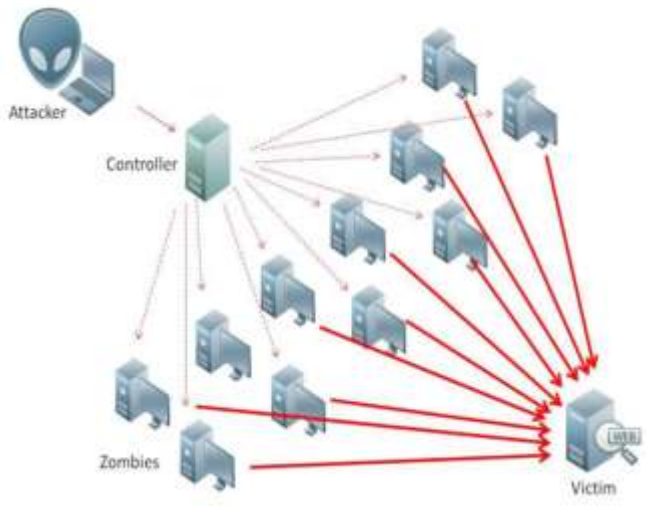

Fig -1: Procedure of DDoS Attack

2. DISTRIBUTED DENIAL OF SERVICE (DDoS) ATTACK TOOLS

Distributed Denial of Service attack region unit underneath presence since center 1980's and region unit still the highest net security danger. The vital reason behind this attack is that the convenience and class of the attack tools. Samples of attack tools area unit: Trinoo, TFN2K, Shaft etc. The attack tools generate UDP Flooding, ICMP Flooding, TCP Flooding, Smurf attack etc.

Table -1: Attack Tools Vs. Attack Type Generated

DDoS ATTACK TOOLS	ATTACK TYPE GENERATED BY THE TOOL
TFN2K	UDP Flooding, TCP Flooding, ICMP Flooding, Smurf
Shaft	UDP Flooding, TCP Flooding, ICMP Flooding,
Stacheldraht	UDP Flooding, TCP Flooding, ICMP Flooding,
Knight	UDP Flooding, TCP Flooding,
Mstream	TCP Flooding,
Trinity	UDP Flooding, TCP Flooding,
Trinoo	UDP Flooding

3. RELATED WORK

Several studies and researches have been reported in the last few years for the detection and classification of DDoS attack by using different classifiers. In year 2015, Bharti Nagpal, Pratima Sharma, Naresh Chauhan and Angel Panesar described the various vulnerable systems on the Internet that can be used for launching DDoS attacks and, DDoS attacks are very difficult to defend against in spite of using defense mechanisms and will be an effective form of attack.

In year 2015, Amey Shevtekar and Nirwan Ansari proposed a new DDoS advance archetypal by application botnets that is evadable and can be calmly mistaken as absolute congestion.

In year 2015, I Gde Dharma N., M. Fiqri Muthohar, Alvin Prayuda J. D., Priagung K. and Deokjai Choi described experiment scenario and also how to appraise the achievement of method

In year 2013, Yuan Tao, and Shui Yu proposed experiments and simulations demonstrate that the proposed apprehension algorithms are able and absolute of advance features.

In year 2012,Alex Doyal, Justin Zhan and Huiming Anna Yu proposed Triple Dos is a DDoS defense adjustment that makes use of absorption at the ancillary of an aerial broadcast arrangement to assure in action to dispensed abnegation of account assaults.

In year 2012,Poongothai, M and Sathyakala, M they do not proposed solutions for the issues discussed in this paper, it's miles vital to recognize and understand trends in attack technology with a view to efficiently and accurately evolve protection and reaction techniques to help examine how protection regulations, processes, and technologies may need to trade to cope with the present day traits in DDoS attack technology.

In year 2009,Ashley Chonka, Jaipal Singh, and Wanlei Zhou proposed the introduced a new algorithm that can adumbrate the attributes of arrangement cartage in a activating system.

In year 2009, Arun Raj Kumar, P. and S. Selvakumar proposed the most popular tools are identified, studied, and compared. DDoS attack happens not only for wired networks but also for wireless environments (where laptops are used as workstations in each site).

In year 2006,Yang Xiang, Wanlei Zhou, and Zhongwen Li proposed an analytical model that can describe the interactions amid the DDoS advance affair and the defense affair according to experiments.

In year 2004, Stephen M. Specht and Ruby B. Lee described approximately DDoS attacks make a networked gadget or service unavailable to legitimate customers. Those attacks are an annoyance at a minimum, or may be critically adverse if a crucial system is the number one sufferer. Loss of community sources causes economic loss, work delays, and loss of verbal exchange between community users. Answers should be advanced to save you those DDoS attacks.

4. PROPOSED METHODOLGY

DDoS advance allocation arrangement consists of 5 above phases, as illustrated in amount 2. File is being collected through the web servers. Through which information is being collected. Distributed Denial of Service attack is being consists of highly damageable threats through which data is not being easily available.

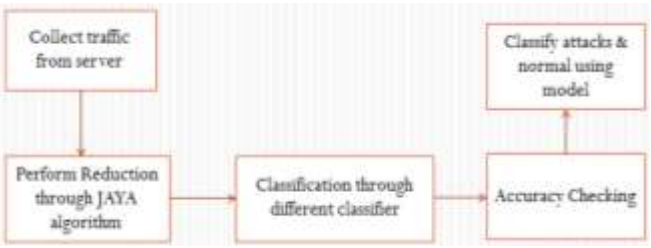

Fig -2: Attack Detection and Classification System

4.1 Reduction

File is being collected from server contains lots of information about legitimate users as well as illegitimate users. Through which it consume lot of time to process the file, for reducing time we use JAYA algorithm through which the data as well time is being reduced.

JAYA Algorithm is acclimated for analytic accountable and airy enhancement problem. It initializes citizenry size, amount of architecture variables and abortion criterion, afterwards that identifies best and affliction solutions in the

citizenry again adapt the Band-Aid based on best and affliction solutions application formula:-

$$X_{id} = X_{id+} r_1(X_{best} - X_{id}) - r_2(X_{worst} - X_{id})$$

After that it checks the Band-Aid is bigger that agate amount if yes afresh acquire and alter the antecedent Band-Aid and if no afresh accumulate the antecedent Band-Aid afterwards that it checks that whether abortion archetype annoyed or not if yes afresh address optimum Band-Aid and if no afresh accomplished action is getting afresh again until abortion archetype satisfied.

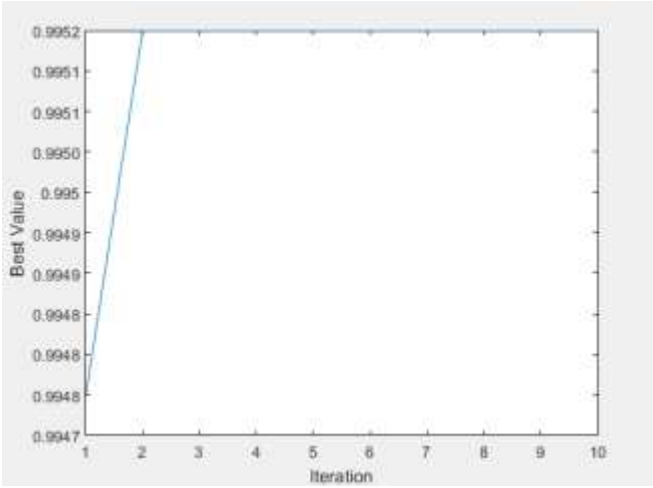

Fig -3: Iterated graph through JAYA algorithm

4.2 Classification with Different Classifiers

Classification is done to check the accuracy rate of data using different classifiers. There are 4 types of classifiers which are divided into sub parts they are as follows:-

- Decision Tree
- Complex Tree
- Medium Tree
- Simple Tree
- Support Vector Machine
- Linear SVM
- Quadratic SVM
- Cubic SVM
- Fine Gaussian SVM
- Medium Gaussian SVM
- Coarse Gaussian SVM
- Nearest Neighbor Classifiers
- Fine KNN
- Medium KNN
- Coarse KNN
- Cosine KNN
- Cubic KNN
- Weighted KNN
- Ensemble Classifiers
- Boosted Tree
- Bagged Tree
- Subspace Discriminant
- Subspace KNN
- RUS Boost

The above mention classifiers is being used for classify data through which the conclusion is that the Bagged Tree Ensemble Classifier gives more accuracy than others.

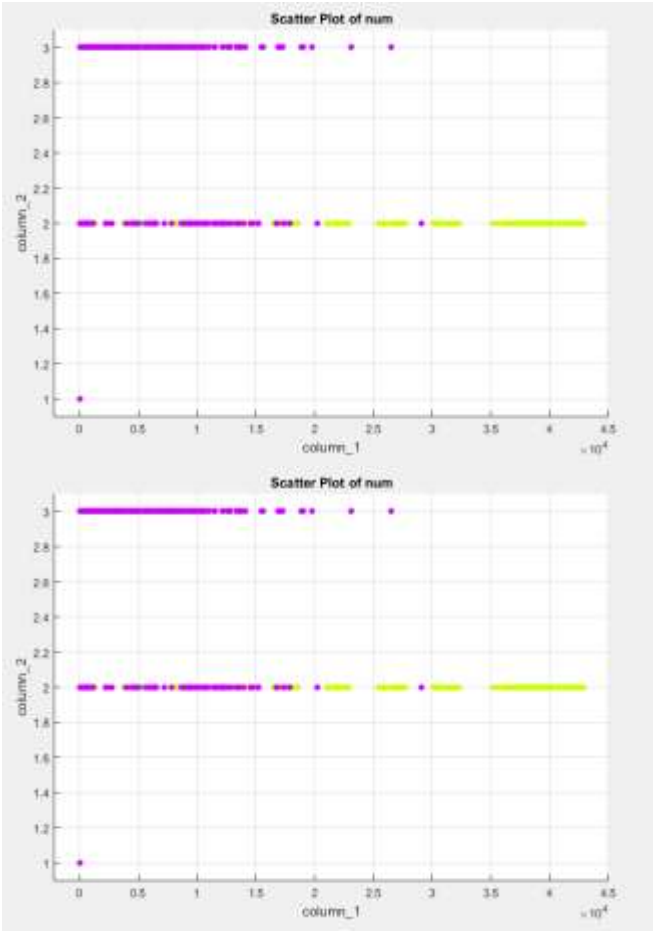

Fig -4: Normal graph

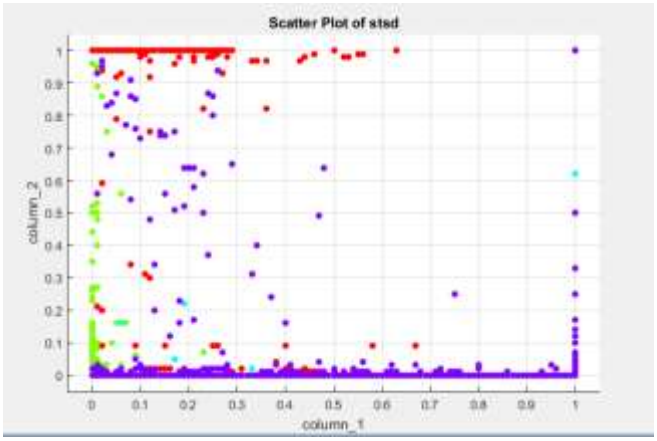

Fig -5: Graph after reduction

5. EXPERIMENTAL RESULT

All the results that are classified that can have a misclassification rate through which accuracy and efficiency will be determined. The graph showing the accuracy level through which we conclude that the Bagged tree Ensemble classifier is accurate as compare to others.

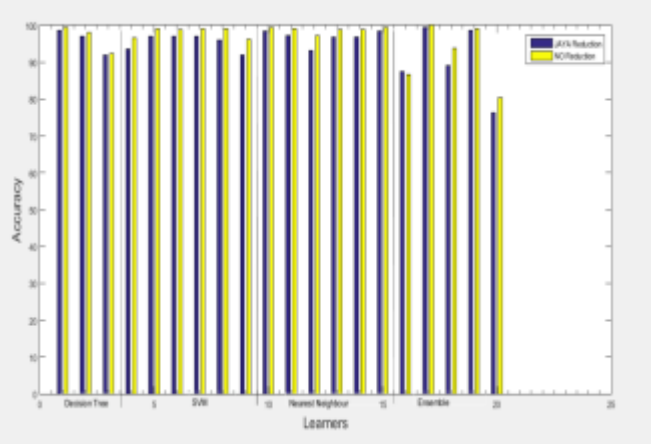

Fig -6: Classification and Accuracy graph

6. CONCLUSIONS

Application layer DDoS attacks are successfully detected and classified by different classifiers through which we come to know that which classifier is best for this condition. JAYA algorithm is used for reduction of data through which attacked and non-attacked data is being differentiated through which reduction of data is being performed. Bagged Tree Ensemble Classifier produce the better classification accuracy as compare to other classifiers. The Bagged Tree Ensemble classifier achieves an accuracy of 99.5%. In future it may work on different layers with new algorithm for reduction of time through which more accuracy may be achieved.

ACKNOWLEDGEMENT

For this paper, a large amount of credit goes to our guide Mr. Vimal Parganiha for his continuous assistance, patience and support.

REFERENCES

[1]. A.Ramamoorthi, T.Subbulakshmi, Dr. S. Mercy Shalinie, "Real Time Detection and classification of DDoS Attacks using Enhanced SVM with String Kernels",ICRTIT 2011 MIT, Anna University, Chennai, June 3-5, 2011.

[2]. R.Venkata Rao, "JAYA:A simple and new optimization algorithm for solving constrained and unconstrained optimization problems", internationaljournal of Industrial Engineering Computations 7(2016) 19-34.

[3]. Qiao Yan, F Richard Yu, Qingxiang Gong and Jianqiang Li, "Software-Defined Networking (SDN) and Distributed Denial of Service (DDoS) Attacks in Cloud Computing Environments: A Survey, Some Research Issues, and Challenges" IEEE 2015.

[4]. I Gde Dharma N.,M. Fiqri Muthohar, Alvin Prayuda J. D., Priagung K., Deokjai Choi, "Time-based DDoS Detection and Mitigation for SDN Controller",IEEE 2015.

[5]. Bharti Nagpal, Pratima Sharma, Naresh Chauhan and Angel Panesar, "DDoS Tools: Classification, Analysis and Comparison" IEEE 2015.

[6]. Bharat Rawal, Anthony Tsetse and Harold Ramcharan, "Emergence of DDoS Resistant Augmented Split Architecture", IEEE 2013.

[7]. YiXie and Shun-Zheng YU, "A large-Scale Hidden Semi-Markov Model for Anomaly Detection on User Browsing Behaviours" IEEE 2009.

[8]. YiXie and Shun-Zheng, "Monitoring the Application layer DDoS Attacks for Popular Websites", IEEE/ACM Trans. On networking, Vol.17, No.1, pp. 15-25, 2009.

[9]. Yoohwan Kim, Wing Cheong Lau, Mooi Choo Chuah and Jonatan Chao "Packet Score: A Statistics-Based Packet Filtering Scheme against DistributedDenial-of-Service Attacks", IEEE Trans. On dependable and secure computing, Vol.3, No. 2, pp. 2594-2604, 2006.

[10]. Amey Shevtekar and Nirwan Ansari, "Is It Congestion or a DDoS Attack?" transaction IEEE communications letters, VOL.13, No. 7, Jul 2009, pp. 546-548.

[11]. Thing, V.L.L. Sloman, M.Dulay, N. "Locating network domain entry and exit point/path for DDoS attack traffic" IEEE Trans. On Networking andService Management, Vol. 6, No.3, pp. 163-170, 2009.

[12]. Chonka, A.singh, J.Wanlei Zhou, "Chaos theory based detection against network mimicking DDoS attacks", IEEE Trans. On Communications Letters,Vol.13, No. 9, pp. 717-721, 2009.

[13]. Arun Raj Kumar, P. and S. Selvakumar, "Distributed Denial of Service (DDoS) Threat in Collaborative Environment-A survey on DDoS Attack Tools and Traceback Mechanisms", International Advance Computing Conference (IACC 2009), pp. 1275-1280, March 2009.

[14]. Poongothai and Sathyakala, "Simulation and Analysis of DDoS Attacks", International Conference on Emerging Trends in Science, Engineering and Technology, pp. 78-85, 2012.

[15]. B. Hancock, "Trinity v3, a DDoS tool", Computer Security, 2000.

[16]. Saman Taghavi Zargar, James joshi and David Tipper, "A Survey of Defense Mechanism Against Distributed Denial of Service (DDoS) Flooding Attacks", IEEE communications Surveys & Tutorials, Vol. 15, No. 4, pp. 2046-2068, 2013.

[17]. Alex Doyal, Justin Zhan and Huiming Anna Yu, "Towards Defeating DDoS Attacks", International Conference on Cyber Security, pp. 209-211, 2012 IEEE.

[18]. Yang Xiang, Wan lei Zhou and Zhongwen Li, "An Analytical Model for DDoS Attacks and Defense", IEEE 2006.

[19]. Soon Hin Khor and Akihiro Nakao, "DaaS: DDoS Mitigation- as – a-Service", IEEE 2011

[20]. Yuan Tao and Shui Yu, "DDoS Attack Detection at Local Area Networks Using Information Theoretical Metrics", IEEE 2013.