Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X
IMPACT FACTOR: 5.258

IJCSMC, Vol. 5, Issue. 3, March 2016, pg.244 – 248

Classification and Detection of Distributed Denial of Service (DDoS) Attack

Rida Anwar[1], Preeti Tuli[2]

[1]Reasearch Scholar, Computer Science Department, CSVTU, Bhilai, India

[2]Reader and Head, Computer Science Department, CSVTU, Bhilai, India

[1] anwarrida09@gmail.com; [2] preeti.tuli@dishamail.com

Abstract— Distributed Denial of Service (DDoS) attack could be a continuous crucial threat to the web. Application layer DDoS attack comes from the lower layers. Application layer based mostly DDoS attacks use legitimate communications protocol requests when institution of communications protocol 3 manner hand shaking and overwhelms the victim resources, like sockets, CPU, memory, disk, database bandwidth. Network layer based mostly DDoS attacks sends the SYN, UDP and ICMP requests to the server and exhausts the bandwidth. Traditional profile is formed from user's access behaviour attributes that is that the final analysis to differentiate DDoS attacks from flash crowd. An anomaly detection mechanism is projected during this paper to detect DDoS attacks .through that traditional user access behaviour attributes.

Keywords— DDoS, Intrusion Detection, Routing Protocol, Enhanced Support Vector Machine, Internet Protocol, DNS.

I. INTRODUCTION

Computer security in the main comprise of confidentiality, integrity and convenience. The foremost threats in security research area unit breach of confidentiality, failure of genuineness and unauthorized DoS. DDoS attack has caused severe damage to servers and can cause even bigger intimidation to the development of recent web services. Historically, DDoS attacks area unit distributed at the network layer, such as ICMP flooding, SYN flooding, and UDP flooding, which are called Network layer DDoS attacks. In Application layer DDoS attacks zombies attack the victim internet servers by protocol GET requests (e.g., protocol Flooding) and propulsion massive image files from the victim server in overwhelming numbers.

In another instance, attackers run a huge range of queries through the victim's program or information question to bring the server down. On the opposite hand, a brand new special phenomenon of network traffic referred to as flash crowd has been noticed by researchers throughout the past many years. On the web, "flash crowd" refers to the case once a really massive number of users at the same time access a preferred site, which produces a surge in traffic to the net web site and would possibly cause the location to be nearly inaccessible. The workability of DDoS Attack is shown in Fig.1.

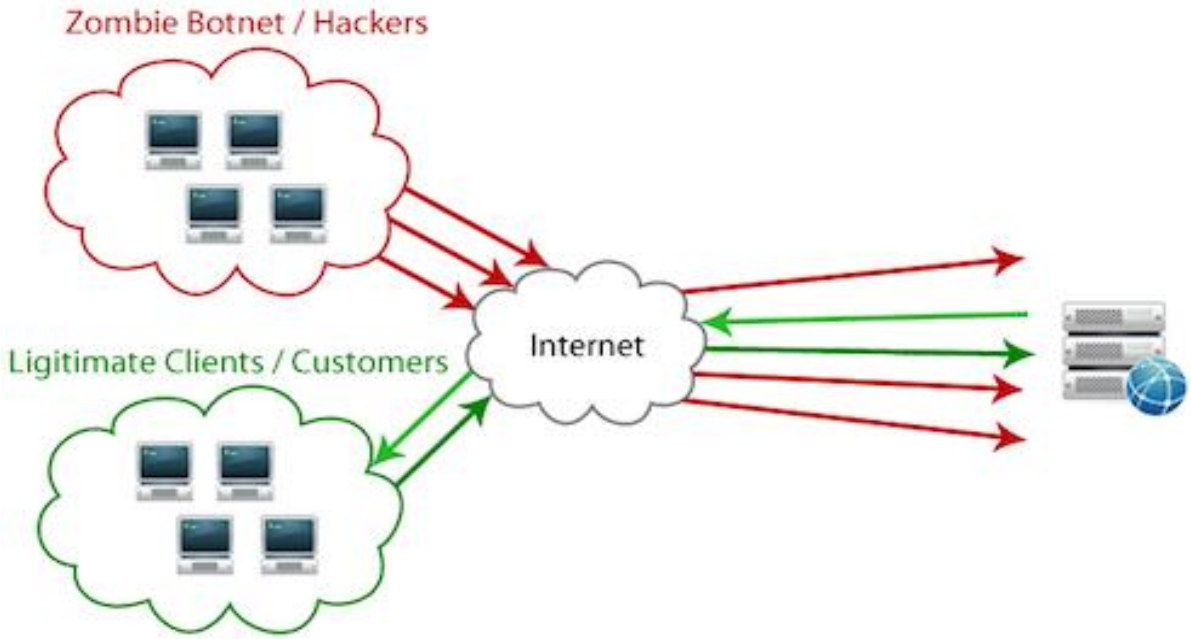

Fig.1.Workability of DDoS Attack

Web user behaviour is principally influenced by the structure of web site and therefore the approach user's access web content. Application layer DDoS attacks square measure thought of as anomaly browsing behaviour and characteristic of net access behaviour is employed to construct the traditional profile that is employed for differentiating attack traffic from traditional traffic. The browsing behaviour of an internet user is expounded to the structure of an internet site, that includes of a large range of web documents, hyperlinks, and therefore the approach the user accesses the WebPages. A typical webpage contains variety of links to other embedded objects, that square measure said as in-line objects. An internet site are often characterised by the hyperlinks among the online pages and therefore the range of in-line objects in each page. Once users click a link inform to a page, the browser can transmit variety of requests for the page and its many in-line objects. Time taken to show the content of the webpage is termed as 'HTTP ON' amount. Time spent by the user to know the content of the page is called 'HTTP OFF'. User might follow a series of hyperlinks provided by this browsing website to continue the access. Throughout traditional user access 'HTTP ON' amount is a smaller amount than the 'HTTP OFF' amount, however throughout Application layer DDoS attack 'HTTP OFF' amount is a smaller amount than the 'HTTP ON' period.

II. DISTRIBUTED DENIAL OF SERVICE (DDOS) ATTACK TOOLS

Distributed Denial of Service attacks area unit underneath existence since middle 1980's and area unit still the upmost net security threat. 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 I
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

III.RELATED WORK

All Several studies and researches have been reported in the last few years for the detection and classification of DDoS attack by extracting different features mentioned in the above section. The work is as follows:

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 defence mechanisms and will be an effective form of attack.

In year 2015,Amey Shevtekar and Nirwan Ansari proposed a new DDoS attack model by using botnets that is evadable and can be easily mistaken as real 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 evaluate the performance of method.

In year 2013,Yuan Tao, and Shui Yu proposed experiments and simulations demonstrate that the proposed detection algorithms are effective and independent of attack features.

In year 2012,Alex Doyal, Justin Zhan and Huiming Anna Yu proposed Triple Dos is a DDoS defence method that makes use of clustering at the side of an overhead relay network to protect in opposition to dispensed denial of service 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 predict the nature of network traffic in a dynamic 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 between the DDoS attack party and the defence party 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 assaults 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.

IV. DDoS DEFENSE TECHNIQUES

Several solutions are planned by numerous researchers to beat DDoS attacks so as to secure the networking atmosphere from malicious attackers. The categories of defence mechanisms are:

A. *Firewall Based Protection*

Until the year 1996, the firewall was the fundamental means that of protection for all forms of network based mostly attacks. Firewalls have straightforward rules, together with to permit or deny protocols, ports or information processing addresses. Firewalls were additionally accustomed mitigate DDoS threats. Bailey et al (1996) planned a technique SYN Defender that protects against the TCP SYN flood assaults by means that of intercepting all SYN packets and mediating the link makes an attempt previous they reach the operative machine.

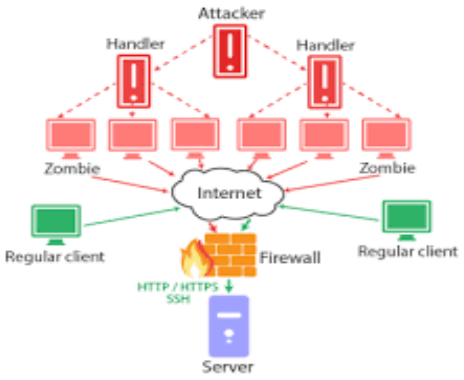

Fig.2. Firewall Based Protection

B. *Active Monitoring*

This class of solutions includes mistreatment software system program marketers to unceasingly chase TCP/IP guests in an exceedingly network at a given neck of the woods. It will anticipate bound conditions to arise and react befittingly. Schuba et al (1997) projected a full of life anomaly detection tool that may detect the condition of SYN flooding attack and react befittingly to defeat, or a minimum of reduce the impact of, an attack. The investigator introduces, "syn skill" that provides safety towards SYN flooding for all hosts connected to the identical neighbourhood region network, impartial in their running contrivance or networking stack implementation.

C. *Overlay Networks*

Here associate degree overlay network is employed to mitigate DDoS threat, wherever associate degree overlay may be a electronic network that designed on prime of another network. Stone (2000) projected associate degree informatics overlay Network for trailing DoS floods referred to as Centre Track. It consists of informatics tunnels or other connections that's wont to by selection routine attention-grabbing datagram's directly from edge routers to special trailing routers

D. *Filtering Mechanism*

These strategies use a way of filtering of the packet supported some filtering rules. If associate degree ISP is aggregating routing announcements for over one downstream networks, strict web {site} guests filtering ought to be accustomed limit site guests, which claims to own originated from out of doors these mass announcements.

E. *Capability Based Approaches*

Capabilities or tokens are utilized in this mechanism for authentication functions associated additionally to classify between a legitimate and an attacker.

F. *Trace back And Pushback Mechanism*

Trace back mechanism concentrates on distinguishing the hosts answerable for associate attack and like offer filtering, will very little to save lots of you source from causation Pushback but employs dynamic website guests filters. Dynamic pushback is employed to stop resource exhaustion. With pushback, node or link characterizes the categories of packets inflicting the flood, and sends request upstream to rate limit them nearer to the supply.

G. *Filtering Capability Approaches*

Capabilities or tokens square measure employed in this mechanism for authentication purpose associate degree additionally to classify between a legitimate and an attacker.

H. *Identification and Classification of Botnet*

Seewald & Gansterer (2009) projected a passive approach to observe and determine the botnets. A passive botnet defence approach is projected at 3 determine the botnets. A passive botnet defence approach is projected at 3 stratified levels, namely the level of one packet, network access and protocol conversations.

I. *Captcha Based Mechanism*

Several works are within the literature that gives associate application level defence mechanism. Google, Yahoo and Hotmail uses text based CAPTCHA (Computer Aided Public Turing Test to tell Computer Human Apart) as associate application level defence mechanism.

V. PROPOSED CLASSIFICATION ALGORITHM

Input: Network Traffic
Output: Classified Instances

1. Begin
2. Collect traffic from server
3. For each Flow
   Get patterns (HTTP request rate, Session rate,
   Page viewing time, Number of TCP packets,
   Number of UDP packets, Number of ICMP
   Packets, Number of Land packets, Protocol)
4. If pattern equals normal flow pattern
   Then
   Assign low weight
5. Else
   Assign high weight
6. Train Enhanced SVM using Training patterns and
   their assigned weight
7. Classify attack classes and normal using model file
8. End

VI. CONCLUSIONS

From the review of the above papers and completely different options, it will be all over that a lot of completely different techniques will be wont to detect Distributed Denial of Service (DDoS) attack completely with different options. DDoS may be a reasonably DOS attack during which multiple compromised systems, that area unit oftentimes infected with a Trojan, area unit wont to goal one machine inflicting a Denial of service (DoS) attack.Hence, the detection must be wiped out its earlier stages. There is a constant research happening in this field. right here, an strive is done to research and apprehend a number of the strategies used until now for the detection and classification of DDoS assault through the usage of proposed algorithms and the methods proposed within the research papers.

ACKNOWLEDGEMENT

For this paper, a large amount of goes to our guide Reader and Head, Dept of C.S.E, Mrs Preeti Tuli. The author is thankful to her for her nonstop help, tolerance and backing in preparation of this paper.

REFERENCES

[1] 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.

[2] 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.

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

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

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

[6] 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.

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

[8] 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.

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

[10] 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.

[11] 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.

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

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

[14] 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.

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

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

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

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

